ID: 652393
Sample Name:
kyFBQxVbsg.exe
Cookbook: default.jbs
Time: 09:43:27
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

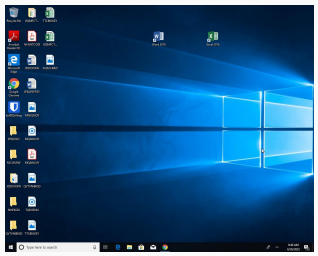
Windows Analysis Report

kyFBQxVbsg.exe

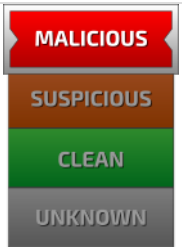
Overview

General Information

Sample Name:	kyFBQxVbsg.exe
Analysis ID:	652393
MD5:	972334f0c55d0a..
SHA1:	e9097b5cd1f976..
SHA256:	eb91bf1e2eb387..
Tags:	exe RAT RemcosRAT
Infos:	



Detection



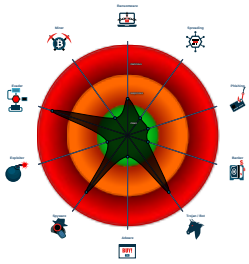
Remcos

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

Signatures

- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Remcos RAT
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for drop…
- Contains functionality to steal Firefo…
- Yara detected Costura Assembly Lo…
- Encrypted powershell cmdline option…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- kyFBQxVbsg.exe (PID: 6232 cmdline: "C:\Users\user\Desktop\kyFBQxVbsg.exe" MD5: 972334F0C55D0AEAB0B32EFE41EA3470)
  - powershell.exe (PID: 6288 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAAMQAwADsAIABTAGUAdAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAGEAdABoACAAJwB DADoAXAAnAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - InstallUtil.exe (PID: 2328 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - InstallUtil.exe (PID: 6528 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Qerdo.exe (PID: 6216 cmdline: "C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe" MD5: 972334F0C55D0AEAB0B32EFE41EA3470)
  - InstallUtil.exe (PID: 2592 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - InstallUtil.exe (PID: 5836 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Qerdo.exe (PID: 5652 cmdline: "C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe" MD5: 972334F0C55D0AEAB0B32EFE41EA3470)
  - InstallUtil.exe (PID: 4900 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - InstallUtil.exe (PID: 6304 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Version": "3.5.1 Pro",
  "Host:Port:Password": "nikahuve.ac.ug:6968:0kalskala.ac.ug:6968:0tuekisaa.ac.ug:6968:0parthaha.ac.ug:6968:0",
  "Assigned name": "06192022",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "cvxyttydfsgbghfgfhtd-RXTSAM",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "scxs.dat",
  "Keylog crypt": "Enable",
  "Hide keylog file": "Enable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "forbas",
  "Keylog file max size": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000000.535499326.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000011.00000000.535499326.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x61100:$s1: \Classes\mscfile\shell\open\command • 0x61160:$s1: \Classes\mscfile\shell\open\command • 0x61148:$s2: eventvwr.exe
00000011.00000000.535499326.0000000000400000.00000040.00000400.00020000.00000000.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x62094:$str_a1: C:\Windows\System32\cmd.exe • 0x62010:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x62010:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x615f8:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x61c50:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x611f4:$str_b2: Executing file: • 0x621d8:$str_b3: GetDirectListeningPort • 0x61a10:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x61c38:$str_b7: \update.vbs • 0x6121c:$str_b9: Downloaded file: • 0x61208:$str_b10: Downloading file: • 0x612ac:$str_b12: Failed to upload file: • 0x621a0:$str_b13: StartForward • 0x621c0:$str_b14: StopForward • 0x61be0:$str_b15: fso.DeleteFile " • 0x61b74:$str_b16: On Error Resume Next • 0x61c10:$str_b17: fso.DeleteFolder " • 0x6129c:$str_b18: Uploaded file: • 0x6125c:$str_b19: Unable to delete: • 0x61ba8:$str_b20: while fso.FileExists(" • 0x61731:$str_c0: [Firefox StoredLogins not found]
00000011.00000000.533973605.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000011.00000000.533973605.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x61100:$s1: \Classes\mscfile\shell\open\command • 0x61160:$s1: \Classes\mscfile\shell\open\command • 0x61148:$s2: eventvwr.exe
Click to see the 97 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.0.InstallUtil.exe.400000.5.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
17.0.InstallUtil.exe.400000.5.raw.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x61100:$s1: \Classes\mscfile\shell\open\command • 0x61160:$s1: \Classes\mscfile\shell\open\command • 0x61148:$s2: eventvwr.exe
17.0.InstallUtil.exe.400000.5.raw.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x62094:$str_a1: C:\Windows\System32\cmd.exe • 0x62010:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x62010:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x615f8:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x61c50:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x611f4:$str_b2: Executing file: • 0x621d8:$str_b3: GetDirectListeningPort • 0x61a10:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x61c38:$str_b7: \update.vbs • 0x6121c:$str_b9: Downloaded file: • 0x61208:$str_b10: Downloading file: • 0x612ac:$str_b12: Failed to upload file: • 0x621a0:$str_b13: StartForward • 0x621c0:$str_b14: StopForward • 0x61be0:$str_b15: fso.DeleteFile " • 0x61b74:$str_b16: On Error Resume Next • 0x61c10:$str_b17: fso.DeleteFolder " • 0x6129c:$str_b18: Uploaded file: • 0x6125c:$str_b19: Unable to delete: • 0x61ba8:$str_b20: while fso.FileExists(" • 0x61731:$str_c0: [Firefox StoredLogins not found]
24.2.Qerdo.exe.5440000.4.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
24.2.Qerdo.exe.5440000.4.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x5b6a2:$s1: file:/// • 0x5b5fe:$s2: {11111-22222-10009-11112} • 0x5b632:$s3: {11111-22222-50001-00000} • 0x58303:$s4: get_Module • 0x5841f:$s5: Reverse • 0x59b22:$s6: BlockCopy • 0x5a1a4:$s7: ReadByte • 0x5b6b6:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
Click to see the 187 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Malware Analysis System Evasion

Delayed program exit found

HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected Remcos RAT

Contains functionality to steal Firefox passwords or cookies

Contains functionality to steal Chrome passwords or cookies

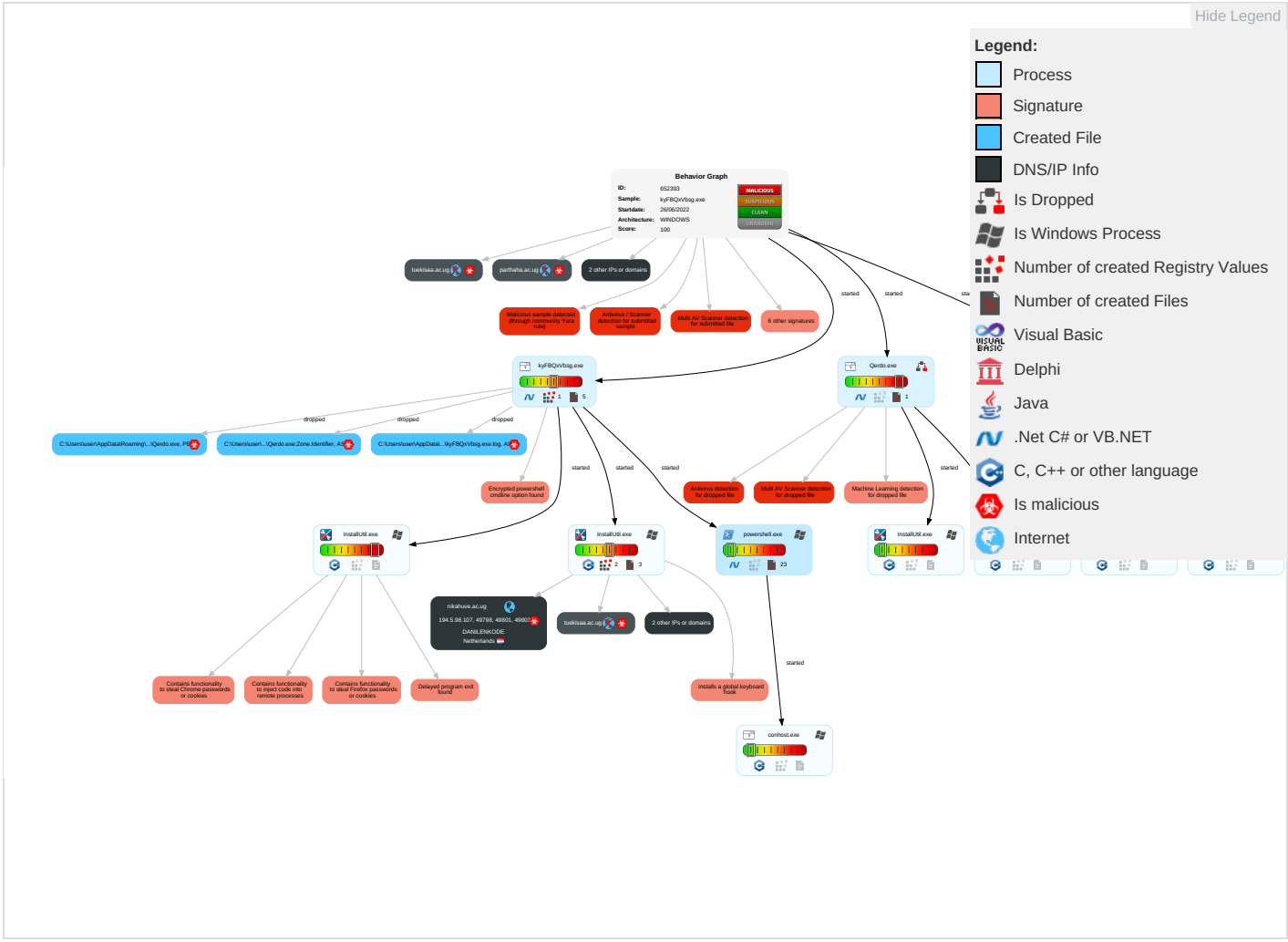
Remote Access Functionality

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Windows Service	1 1 Deobfuscate/Decode Files or Information	1 2 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	1 2 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Service Execution	Logon Script (Windows)	1 2 2 Process Injection	3 Obfuscated Files or Information	2 Credentials In Files	1 System Service Discovery	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 PowerShell	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 3 Software Packing	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	3 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 2 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	2 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 2 Process Injection	Proc Filesystem	3 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

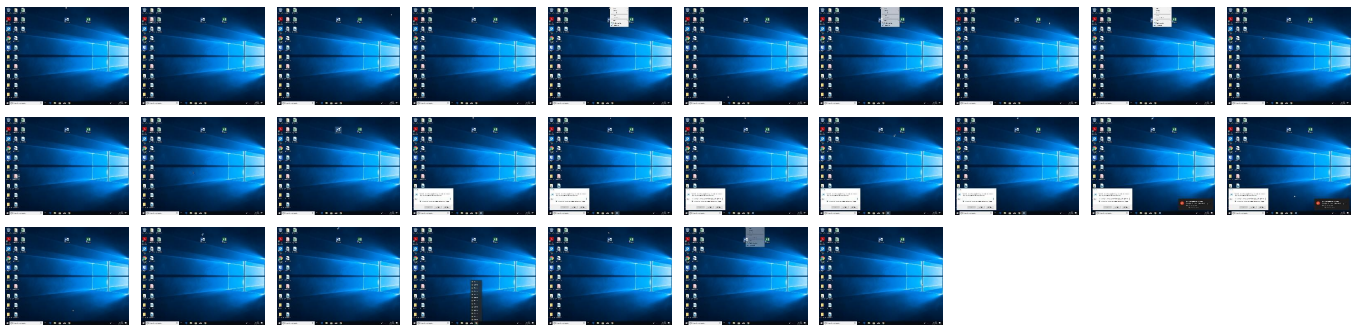
Behavior Graph



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
kyFBQxVbsg.exe	46%	Virustotal		Browse
kyFBQxVbsg.exe	58%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
kyFBQxVbsg.exe	100%	Avira	TR/Dropper.MSIL.Gen	
kyFBQxVbsg.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe	58%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
26.2.InstallUtil.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.InstallUtil.exe.400000.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.InstallUtil.exe.400000.7.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.8.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
0.2.kyFBQxVbsg.exe.2e0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
28.0.InstallUtil.exe.400000.5.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.InstallUtil.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.3.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.4.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
19.2.Qerdo.exe.40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
28.0.InstallUtil.exe.400000.3.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.7.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.0.InstallUtil.exe.400000.7.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.InstallUtil.exe.400000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.6.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
19.0.Qerdo.exe.40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
28.2.InstallUtil.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.0.InstallUtil.exe.400000.4.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.0.InstallUtil.exe.400000.5.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.0.InstallUtil.exe.400000.6.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
24.2.Qerdo.exe.9a0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
28.0.InstallUtil.exe.400000.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.InstallUtil.exe.400000.8.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
24.0.Qerdo.exe.9a0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
26.0.InstallUtil.exe.400000.5.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.2.InstallUtil.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
0.0.kyFBQxVbsg.exe.2e0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
17.0.InstallUtil.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.0.InstallUtil.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.InstallUtil.exe.400000.6.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.InstallUtil.exe.400000.4.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.0.InstallUtil.exe.400000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.0.InstallUtil.exe.400000.8.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
26.0.InstallUtil.exe.400000.3.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
nikahuve.ac.ug	4%	Virustotal		Browse
tuekisaa.ac.ug	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gp	0%	URL Reputation	safe	
http://geoplugin.net/json.gp/C	0%	URL Reputation	safe	
nikahuve.ac.ug	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nikahuve.ac.ug	194.5.98.107	true	true	• 4%, Virustotal, Browse	unknown
tuekisaa.ac.ug	unknown	unknown	true	• 2%, Virustotal, Browse	unknown
parthaha.ac.ug	unknown	unknown	true		unknown
kalskala.ac.ug	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nikahuve.ac.ug	true	• Avira URL Cloud: safe	unknown

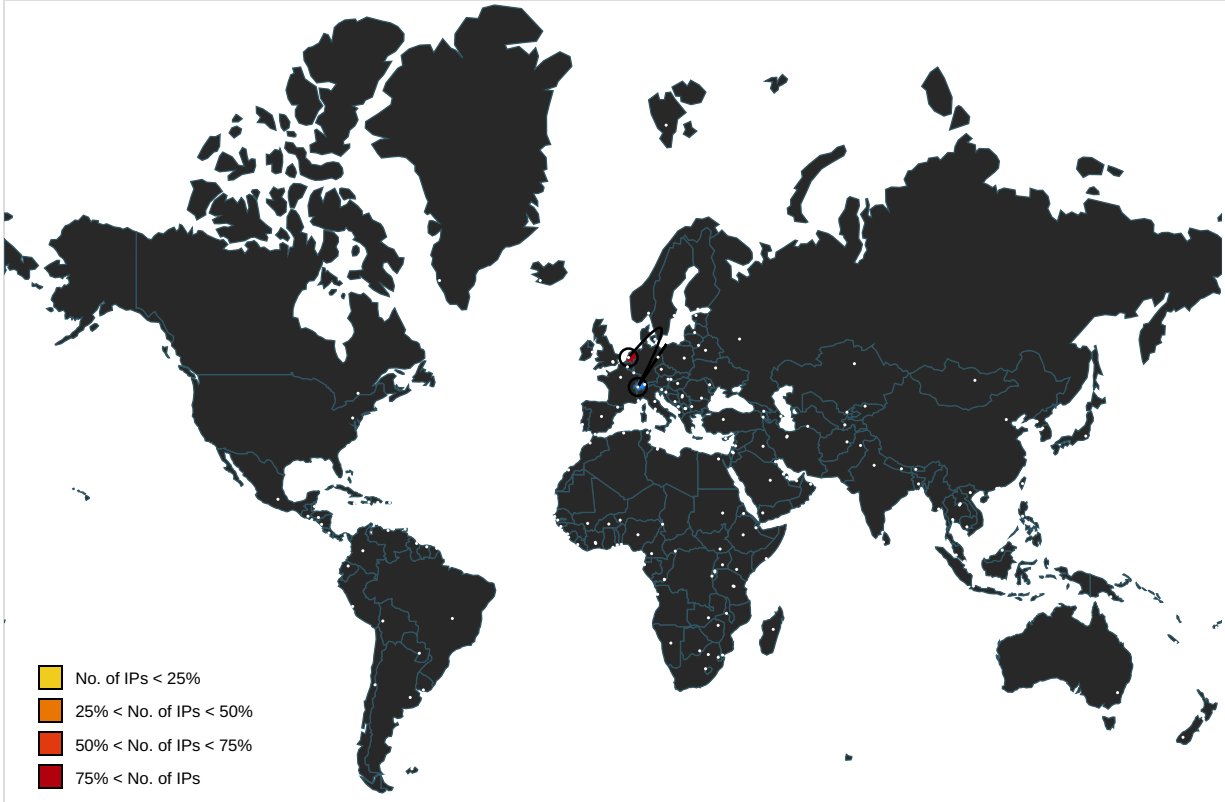
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://geoplugin.net/json.gp	InstallUtil.exe	false	• URL Reputation: safe	unknown
http://https://github.com/mgravell/protobuf-net	kyFBQxVbsg.exe, 00000000.00000003.526677018.000000000398E000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000003.526824087.0000000003A06000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582007777.000000000368E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582307729.0000000003706000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588674839.000000000419E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588792827.0000000004216000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-neti	kyFBQxVbsg.exe, 00000000.00000003.526677018.000000000398E000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000003.526824087.0000000003A06000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582007777.000000000368E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582307729.0000000003706000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588674839.000000000419E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588792827.0000000004216000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/q/14436606/23354	kyFBQxVbsg.exe, 00000000.00000002.540068634.000000000269C000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000003.526677018.000000000398E000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000003.526824087.0000000003A06000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000002.597952189.000000000239C000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582007777.000000000368E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582307729.0000000003706000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588674839.000000000419E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000002.610776047.0000000002EAC000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588792827.0000000004216000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-netJ	kyFBQxVbsg.exe, 00000000.00000003.526677018.000000000398E000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000003.526824087.0000000003A06000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582007777.0000000368E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582307729.0000000003706000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588674839.000000000419E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588792827.0000000004216000.00000004.00000800.00020000.00000000.sdmp	false		high
http://geoplugin.net/json.gp/C	kyFBQxVbsg.exe, 00000000.00000002.541310066.000000000382F000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000002.541421315.00000000038CF000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000000.535499326.0000000000400000.00000040.00000400.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000000.533640248.0000000000400000.00000040.00000400.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.645272430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000002.603389337.000000000352F000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000002.605837275.00000000035CF000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000002.612287399.00000000040DF000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000002.612156985.000000000403F000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00001A.00000000.594041394.0000000000400000.00000040.00000400.00020000.00000000.sdmp, InstallUtil.exe, 0000001A.00000000.591921739.0000000000400000.00000040.00000400.00020000.00000000.sdmp, InstallUtil.exe, 0000001A.00000002.595851570.0000000000400000.00000040.00000400.00020000.00000000.sdmp, InstallUtil.exe, 0000001C.00000000.601490372.0000000000400000.00000040.00000400.00020000.00000000.sdmp, InstallUtil.exe, 0000001C.00000002.607934228.0000000000400000.00000040.00000400.00020000.00000000.sdmp, InstallUtil.exe, 0000001C.00000000.598510412.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	kyFBQxVbsg.exe, 00000000.00000002.540068634.000000000269C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/q/11564914/23354;	kyFBQxVbsg.exe, 00000000.00000003.526677018.000000000398E000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000003.526824087.0000000003A06000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582007777.00000000368E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582307729.0000000003706000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588674839.000000000419E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588792827.0000000004216000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/2152978/23354	kyFBQxVbsg.exe, 00000000.00000003.526677018.000000000398E000.00000004.00000800.00020000.00000000.sdmp, kyFBQxVbsg.exe, 00000000.00000003.526824087.0000000003A06000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582007777.00000000368E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000013.00000003.582307729.0000000003706000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588674839.000000000419E000.00000004.00000800.00020000.00000000.sdmp, Qerdo.exe, 00000018.00000003.588792827.0000000004216000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.107	nikahuve.ac.ug	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652393
Start date and time: 26/06/202209:43:27	2022-06-26 09:43:27 +02:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kyFBQxVbsg.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@18/10@117/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 39.4% (good quality ratio 37.4%) • Quality average: 83.7% • Quality standard deviation: 26.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target powershell.exe, PID 6288 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:45:12	API Interceptor	38x Sleep call for process: powershell.exe modified
09:45:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Qerdo "C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe"
09:46:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Qerdo "C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Qerdo.exe.log

Process:	C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	805
Entropy (8bit):	5.360596073797118
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhIE4K5AE4Kzr7r1qE4j:MxHKXwYHKhQnoIHK5AHKzvr1qHj
MD5:	EBFA21D930F1B37DA9DDD9D7E276F9DE
SHA1:	E97B403CAA3A03D0E8BDAC6E66FFBE47555A38E5
SHA-256:	5B9B2A9380AFEBEC985FA5745B9354DBBD4C889542B3EFE5446D24E8430A3752
SHA-512:	13D58B48DB79A6D8A8851186ECD309BB22B859D1FC064B8E05108378F06A71110A1AAE5622E4C61DA201192809BE4910B86037BFC2E4F4261942D6E3EC11DC1
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kyFBQxVbsg.exe.log

Process:	C:\Users\user\Desktop\kyFBQxVbsg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	805
Entropy (8bit):	5.360596073797118
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhIE4K5AE4Kzr7r1qE4j:MxHKXwYHKhQnoIHK5AHKzvr1qHj
MD5:	EBFA21D930F1B37DA9DDD9D7E276F9DE
SHA1:	E97B403CAA3A03D0E8BDAC6E66FFBE47555A38E5
SHA-256:	5B9B2A9380AFEBEC985FA5745B9354DBBD4C889542B3EFE5446D24E8430A3752
SHA-512:	13D58B48DB79A6D8A8851186ECD309BB22B859D1FC064B8E05108378F06A71110A1AAE5622E4C61DA201192809BE4910B86037BFC2E4F4261942D6E3EC11DC1
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:wZvOdB8Ypib4JNXp59HopbjvwRjdvRlAYotiQ0HzAF8:UvOdB8YNNZjHopbjoRjdvRlAYotinHzr
MD5:	C5A56B913DEEDCF5AE01A2D4F8AA69CE
SHA1:	C91D19BFD666FDD02B0739893833D4E1C0316511
SHA-256:	1C5C865E5A98F33E277A81FCDADFBAB1367176BA14F8590022F7E5880161C00D
SHA-512:	1058802FCD54817359F84977DD26AD4399C572910E67114F70B024EBADDF4E35E6AFF6461F90356205228B4B860E69392ABC27D38E284176C699916039CFA5ED
Malicious:	false
Preview:	PSMODULECACHE.....#y;...Q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1.....Start-BitsTransfer.....Set-BitsTransfer .....Get-BitsTransfer.....Resume-BitsTransfer.....Add-BitsFile.....Suspend-BitsTransfer.....Complete-BitsTransfer.....Remove-BitsTransfer.....-.^(...[...C:\Win dows\system32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1....#...Set-AppBackgroundTaskResourcePolicy.....Unregister-App BackgroundTask.....Get-AppBackgroundTask.....tid.....pfn.....iru....%...Enable-AppBackgroundTaskDiagnosticLog.....Start-AppBackgroundTask....&...Disable-Ap pBackgroundTaskDiagnosticLog.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1..... ..Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Pac kage.....Unins

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22176
Entropy (8bit):	5.601138309758725
Encrypted:	false
SSDEEP:	384:5tCABCmzRYPvYAnISBKnLul/sp6vz1Nnqa9ZFtPV7I1WDuZ1v1I5+yYs:VgvBl4KLulcl7qOXNUvr+
MD5:	EA4826E83AF1B21101CE6F68EF0B55C6
SHA1:	0046E23F0CC87039F220713239AD6B86DE91ABF0
SHA-256:	279B8D0ADA726FE5DFB5E6A238E2FFD2FE1A16F971BCFB6B41E4034E0CB9AA88
SHA-512:	39BCC0A6DEA0B45B877F6DCEE5930E34C49B5034F56D0E08168CC525631DE76772ADA7DE79B28263240D4422AB47AF91E9A8917548E10224194D7B924D4C53E B
Malicious:	false
Preview:	@...e.....`.....>.3.0.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_esjq1xkt.ffx.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pshfc5wv.vht.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe

Process:	C:\Users\user\Desktop\kyFBQxVbsg.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	735232
Entropy (8bit):	7.987468698438195
Encrypted:	false
SSDEEP:	12288:9IxCLALqCddwA7Pljw5ej79G72AUBV3xaTPqfH0pLbwfBnC7aCNsuAIi6:9IxAgWA79Mq7s7ZUFV/IwfKagsWi6
MD5:	972334F0C55D0AEAB0B32EFE41EA3470
SHA1:	E9097B5CD1F976ECAF0ACCEDF14F1D22BD72E6FA
SHA-256:	EB91BF1E2EB3877F0942CEF113BB0FB76E2C2FD2C2651DBF09F6DA6DF649E8FB
SHA-512:	DF120F43FA17B2C37AD6D31E528495241146420CD017C18116BD074498CEF3834F408C50D289F8BDCE2955C464664A6C446800CB7B55C1461FB3CC0ACCC7FE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 58%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..b.....0.....F..... .....@.. ....`.....O... ...D..... ..... ..H.....text..... ..... ..`.rsrc....D... ...D.....@..@.reloc..... .....6.....@..B.....H.....$$.....".(....*".(....*...0..g.....s.....s.....s....s.....+..+.o....+....+..o....+.,.+....o.....+..o....+.,. +....,..o.....*..(...../.....:I.....RZ.....0.."..... .....%....(.....(....+..*...0..L.....s.....o.....s.....o.....o.....!.,..o.....,..o.....,..o.....*.(.....).....$4.....8?.....0..`. .....(....(....o....(...+o.....+"..(.....o...

C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\kyFBQxVbsg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\forbas\scxs.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	7.177722839093587
Encrypted:	false
SSDEEP:	6:6p288ILJoF861v83dMuVm6IRRqG6Q6P9SR2p6:6F8ILJoF8cv83uBRp6Qe9a2p6
MD5:	0BC4CF36ABF59CC54AA5D472D55FAE99
SHA1:	FE3A6EB4A46CA56C855CA308EC96838C96C63AA2
SHA-256:	9E6854C21A182D3224B40053CEE8BCF8C6E055C08D7ECE2ED6CDD6F7090C048E

SHA-512:	07028E2E89213CCB36A06968692D22F37452E22920C12B00C2B9503F22906388D1B1B07AAE92C43D675DD82C9BD2B019E53A298B23CEBEE26800B02855595FC6
Malicious:	false
Preview:	.j.V.J..!kU_..sY.[.t.....]..%...*!.A].y..x.....L.B.....C.....=&f&..Vn.}...$.P....{j.gl.....Ni:.o.s./.=...fL...c..<.A..V1...4X>.".|.`....C..m7[u....$F')5..d..p;....2....MB.$..-..{o|{!uc..B.}...m ....X8.0.....7.@.....

C:\Users\user\Documents\20220626\PowerShell_transcript.128757.EFYe5VSb.20220626094450.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5978
Entropy (8bit):	5.485342256824624
Encrypted:	false
SSDEEP:	96:BZ2TLZ+N3azqDo1ZVZVTLZ+N3azqDo1ZXvZprZkTLZ+N3azqDo1Z2wTTyZh:3acaJaq
MD5:	34326C020EA634E84A3536E82DAFA6F8
SHA1:	A2C2D2F602436AC220AE61B1F43ECBE10DFE8292
SHA-256:	4DB38969B245E4F1E94BFE1254F2A77D386F07717A5D61F7B964F4F3D091C8B0
SHA-512:	476601D408665AFBD80DFDE04925C9035E1FF99EAEBE0BBFD33AC61E67FA53977F87E0BEF0C3F7FA210B724D6FB12162690E3C89D2C83A04DCF4DC71B16CBA 21
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220626094508..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -enc UwB0AGEAcgB0 AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMQAwADsAIABTAGUAdAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYw BsAHUAcwBpAG8AbgBQAGEAdABoACAAJwBDADoAXAAnAA==..Process ID: 6288..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220626094509..**********..PS>Start-Sleep -Seconds 10; Set-MpPreference -Ex clusionPath 'C:\'..**********..Windows PowerShell transcript start..Start

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.987468698438195
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	kyFBQxVbsg.exe
File size:	735232
MD5:	972334f0c55d0aeab0b32efe41ea3470
SHA1:	e9097b5cd1f976ecaf0accedf14f1d22bd72e6fa
SHA256:	eb91bf1e2eb3877f0942cef113bb0fb76e2c2fd2c2651dbf09f6da6df649e8fb
SHA512:	df120f43fa17b2c37ad6d31e528495241146420cd017c18116bd074498cef3834f408c50d289f8bdce2955c464664a6c446800cb7b55c1461fb3cc0accc7fe10
SSDEEP:	12288:9IxCLALqCddwA7Pljw5ej79G72AUBV3xaTPqfH0pLbwfBnC7aCNsuAIi6:9IxAgWA79Mq7s7ZUFV/IwfKagsWi6
TLSH:	67F423A18A0BDF5FE18F5ABB680452F7145CFE231240A318BA4173FE2EB354165E77A4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..b.....0.....F..... .....@.. .....`.....

File Icon

Icon Hash:	e4d8d8d8dc483196

Static PE Info

General

Entrypoint:	0x4b0ede
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62B71A23 [Sat Jun 25 14:22:27 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb0e8c	0x4f	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb2000	0x4400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xaeee4	0xaf000	False	0.9951590401785714	data	7.9984009418791	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb2000	0x4400	0x4400	False	0.5211971507352942	data	5.8634338520962395	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb2160	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb26d8	0x1e0b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb44f4	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb4dac	0xea8	data		
RT_GROUP_ICON	0xb5c64	0x3e	data		
RT_VERSION	0xb5cb4	0x362	data		
RT_MANIFEST	0xb6028	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 167

- 53 (DNS)
- 6968 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:45:59.625091076 CEST	49798	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:45:59.667900085 CEST	6968	49798	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:00.312700987 CEST	49798	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:00.355405092 CEST	6968	49798	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:00.919429064 CEST	49798	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:00.964056969 CEST	6968	49798	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:03.523972988 CEST	49801	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:03.566504955 CEST	6968	49801	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:04.126405954 CEST	49801	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:04.168970108 CEST	6968	49801	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:04.811012983 CEST	49801	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:04.854006052 CEST	6968	49801	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:07.212428093 CEST	49803	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:07.255331993 CEST	6968	49803	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:07.837601900 CEST	49803	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:07.880376101 CEST	6968	49803	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:08.428515911 CEST	49803	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:08.471122980 CEST	6968	49803	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:10.571124077 CEST	49805	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:10.613929987 CEST	6968	49805	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:11.219929934 CEST	49805	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:11.262623072 CEST	6968	49805	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:11.811450958 CEST	49805	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:11.856297016 CEST	6968	49805	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:14.949017048 CEST	49809	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:14.993516922 CEST	6968	49809	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:15.610732079 CEST	49809	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:15.653306007 CEST	6968	49809	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:16.219952106 CEST	49809	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:16.262541056 CEST	6968	49809	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:18.189363003 CEST	49814	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:18.235021114 CEST	6968	49814	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:18.923306942 CEST	49814	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:18.967184067 CEST	6968	49814	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:19.610862970 CEST	49814	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:19.653702974 CEST	6968	49814	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:21.858103037 CEST	49830	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:21.900697947 CEST	6968	49830	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:22.532982111 CEST	49830	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:22.575666904 CEST	6968	49830	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:23.126782894 CEST	49830	6968	192.168.2.6	194.5.98.107

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:46:23.169462919 CEST	6968	49830	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:24.980937004 CEST	49846	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:25.027003050 CEST	6968	49846	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:25.567730904 CEST	49846	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:25.610308886 CEST	6968	49846	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:26.127068043 CEST	49846	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:26.172544956 CEST	6968	49846	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:27.845377922 CEST	49859	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:27.888818979 CEST	6968	49859	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:28.424082041 CEST	49859	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:28.468168974 CEST	6968	49859	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:29.111676931 CEST	49859	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:29.154382944 CEST	6968	49859	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:31.270693064 CEST	49864	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:31.317832947 CEST	6968	49864	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:31.924412966 CEST	49864	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:31.967787981 CEST	6968	49864	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:32.612035990 CEST	49864	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:32.657620907 CEST	6968	49864	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:34.441975117 CEST	49866	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:34.488702059 CEST	6968	49866	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:35.127840042 CEST	49866	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:35.170638084 CEST	6968	49866	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:35.737322092 CEST	49866	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:35.783057928 CEST	6968	49866	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:37.239804983 CEST	49867	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:37.285552025 CEST	6968	49867	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:37.799927950 CEST	49867	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:37.842793941 CEST	6968	49867	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:38.346894026 CEST	49867	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:38.391542912 CEST	6968	49867	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:40.412826061 CEST	49868	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:40.455522060 CEST	6968	49868	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:40.956468105 CEST	49868	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:41.001518011 CEST	6968	49868	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:41.503704071 CEST	49868	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:41.548046112 CEST	6968	49868	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:43.088099957 CEST	49870	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:43.130824089 CEST	6968	49870	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:43.644164085 CEST	49870	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:43.690030098 CEST	6968	49870	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:44.191082954 CEST	49870	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:44.235831976 CEST	6968	49870	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:45.616626024 CEST	49871	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:45.663141966 CEST	6968	49871	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:46.175681114 CEST	49871	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:46.222079992 CEST	6968	49871	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:46.722542048 CEST	49871	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:46.767266035 CEST	6968	49871	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:48.412889957 CEST	49873	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:48.456914902 CEST	6968	49873	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:49.097759962 CEST	49873	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:49.142527103 CEST	6968	49873	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:49.691560984 CEST	49873	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:49.735557079 CEST	6968	49873	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:51.152981997 CEST	49874	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:51.197582960 CEST	6968	49874	194.5.98.107	192.168.2.6
Jun 26, 2022 09:46:51.895008087 CEST	49874	6968	192.168.2.6	194.5.98.107
Jun 26, 2022 09:46:51.940021992 CEST	6968	49874	194.5.98.107	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:45:59.455624104 CEST	62643	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:45:59.609529972 CEST	53	62643	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:00.972532034 CEST	54015	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:01.287909031 CEST	53	54015	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:01.302423000 CEST	54489	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:01.668832064 CEST	53	54489	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:01.692954063 CEST	52698	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:02.335402966 CEST	53	52698	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:03.387541056 CEST	61901	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:03.521174908 CEST	53	61901	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:04.861490011 CEST	58689	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:05.224469900 CEST	53	58689	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:05.263015985 CEST	50081	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:05.407883883 CEST	53	50081	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:05.412870884 CEST	49520	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:05.879934072 CEST	53	49520	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:06.900013924 CEST	65526	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:07.183330059 CEST	53	65526	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:08.484833956 CEST	52965	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:08.825110912 CEST	53	52965	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:08.830322981 CEST	52125	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:09.151824951 CEST	53	52125	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:09.172702074 CEST	63104	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:09.415802002 CEST	53	63104	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:10.499820948 CEST	55083	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:10.522844076 CEST	53	55083	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:12.819227934 CEST	58360	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:13.254749060 CEST	53	58360	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:13.285218000 CEST	59724	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:13.417113066 CEST	53	59724	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:13.464816093 CEST	56071	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:13.861335993 CEST	53	56071	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:14.922063112 CEST	60238	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:14.943308115 CEST	53	60238	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:16.272790909 CEST	61152	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:16.600392103 CEST	53	61152	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:16.648164988 CEST	49679	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:16.668729067 CEST	53	49679	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:16.694027901 CEST	60361	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:17.050290108 CEST	53	60361	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:18.078138113 CEST	64579	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:18.172508955 CEST	53	64579	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:19.661204100 CEST	49463	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:19.946038008 CEST	53	49463	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:19.972764015 CEST	55342	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:20.489490032 CEST	53	55342	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:20.527023077 CEST	62041	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:20.808574915 CEST	53	62041	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:21.836281061 CEST	62483	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:21.855746031 CEST	53	62483	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:23.232126951 CEST	55788	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:23.251566887 CEST	53	55788	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:23.258554935 CEST	62448	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:23.277683020 CEST	53	62448	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:23.283349037 CEST	58563	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:23.900996923 CEST	53	58563	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:24.919173002 CEST	57422	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:46:24.938805103 CEST	53	57422	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:26.186084986 CEST	64375	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:26.206334114 CEST	53	64375	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:26.214508057 CEST	63844	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:26.233730078 CEST	53	63844	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:26.238574028 CEST	57269	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:26.787453890 CEST	53	57269	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:27.820296049 CEST	49287	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:27.842549086 CEST	53	49287	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:29.162329912 CEST	64442	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:29.182220936 CEST	53	64442	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:29.200381994 CEST	56146	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:29.220069885 CEST	53	56146	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:29.253309011 CEST	50520	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:29.535430908 CEST	53	50520	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:31.247152090 CEST	56845	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:31.267640114 CEST	53	56845	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:32.667778969 CEST	55300	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:33.007348061 CEST	53	55300	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:33.015280008 CEST	51853	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:33.037226915 CEST	53	51853	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:33.043329000 CEST	62417	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:33.318209887 CEST	53	62417	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:34.348625898 CEST	62834	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:34.429868937 CEST	53	62834	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:35.806056023 CEST	61037	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:35.827079058 CEST	53	61037	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:35.834036112 CEST	58053	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:35.855199099 CEST	53	58053	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:35.862826109 CEST	56031	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:36.128879070 CEST	53	56031	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:37.149254084 CEST	58054	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:37.234436989 CEST	53	58054	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:38.397241116 CEST	59374	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:38.417606115 CEST	53	59374	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:38.421745062 CEST	49815	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:38.926244020 CEST	53	49815	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:38.943577051 CEST	52277	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:39.367716074 CEST	53	52277	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:40.389466047 CEST	49572	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:40.409852028 CEST	53	49572	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:41.557739019 CEST	56949	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:41.579132080 CEST	53	56949	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:41.592691898 CEST	61041	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:41.702279091 CEST	53	61041	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:41.707015991 CEST	54749	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:42.044704914 CEST	53	54749	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:43.057265997 CEST	53169	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:43.077081919 CEST	53	53169	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:44.241111040 CEST	57179	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:44.260705948 CEST	53	57179	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:44.268326998 CEST	55331	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:44.287756920 CEST	53	55331	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:44.291924953 CEST	64325	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:44.559916019 CEST	53	64325	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:45.588435888 CEST	58468	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:45.608629942 CEST	53	58468	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:46.926189899 CEST	56984	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:46.948671103 CEST	53	56984	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:46:46.956815958 CEST	51640	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:46.984714985 CEST	53	51640	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:47.045470953 CEST	63852	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:47.373270035 CEST	53	63852	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:48.388694048 CEST	54570	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:48.407943964 CEST	53	54570	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:49.737145901 CEST	56793	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:49.756731033 CEST	53	56793	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:49.759732962 CEST	61651	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:49.778947115 CEST	53	61651	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:49.780446053 CEST	59925	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:50.115060091 CEST	53	59925	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:51.131019115 CEST	61236	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:51.151547909 CEST	53	61236	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:52.489573956 CEST	49811	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:52.510042906 CEST	53	49811	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:52.512449980 CEST	62639	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:52.535131931 CEST	53	62639	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:52.536928892 CEST	54945	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:52.786977053 CEST	53	54945	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:53.803354025 CEST	59603	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:53.820684910 CEST	53	59603	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:54.972790003 CEST	56939	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:54.992006063 CEST	53	56939	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:54.994334936 CEST	57059	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:55.012367964 CEST	53	57059	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:55.015356064 CEST	54647	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:55.273374081 CEST	53	54647	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:56.287367105 CEST	58490	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:56.363706112 CEST	53	58490	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:57.506583929 CEST	56465	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:57.528808117 CEST	53	56465	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:57.533893108 CEST	61436	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:57.558281898 CEST	53	61436	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:57.560184956 CEST	57048	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:57.833945036 CEST	53	57048	8.8.8.8	192.168.2.6
Jun 26, 2022 09:46:58.850754976 CEST	54558	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:46:58.872860909 CEST	53	54558	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:00.019772053 CEST	56333	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:00.037149906 CEST	53	56333	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:00.040926933 CEST	59824	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:00.062521935 CEST	53	59824	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:00.064255953 CEST	61328	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:00.309726000 CEST	53	61328	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:01.320076942 CEST	50959	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:01.341156960 CEST	53	50959	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:02.488662004 CEST	59344	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:02.832598925 CEST	53	59344	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:02.834417105 CEST	55403	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:02.853538036 CEST	53	55403	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:02.855746984 CEST	58938	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:03.110609055 CEST	53	58938	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:04.116741896 CEST	56625	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:04.133922100 CEST	53	56625	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:05.284356117 CEST	57731	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:05.592148066 CEST	53	57731	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:05.593838930 CEST	49282	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:05.879611015 CEST	53	49282	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:06.250915051 CEST	60760	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:47:06.517442942 CEST	53	60760	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:07.654623985 CEST	64941	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:07.788269043 CEST	53	64941	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:08.926732063 CEST	53690	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:09.216793060 CEST	53	53690	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:09.218846083 CEST	62723	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:09.236004114 CEST	53	62723	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:09.238074064 CEST	55760	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:09.571846008 CEST	53	55760	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:10.585858107 CEST	65452	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:10.603106976 CEST	53	65452	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:11.740303040 CEST	62079	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:12.141793966 CEST	53	62079	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:12.144227982 CEST	51566	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:12.163436890 CEST	53	51566	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:12.167809010 CEST	50050	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:12.589550972 CEST	53	50050	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:13.602176905 CEST	59439	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:13.621402979 CEST	53	59439	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:14.769234896 CEST	64529	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:14.788824081 CEST	53	64529	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:14.792699099 CEST	56759	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:15.098356962 CEST	53	56759	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:15.100631952 CEST	65252	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:15.432835102 CEST	53	65252	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:16.445960999 CEST	65250	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:16.467267990 CEST	53	65250	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:17.613542080 CEST	60801	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:17.630446911 CEST	53	60801	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:17.632636070 CEST	60446	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:17.920314074 CEST	53	60446	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:17.922254086 CEST	51671	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:18.181885004 CEST	53	51671	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:19.196216106 CEST	50442	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:19.217360020 CEST	53	50442	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:20.366450071 CEST	53314	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:20.387876034 CEST	53	53314	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:20.390060902 CEST	61516	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:20.411376953 CEST	53	61516	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:20.413465977 CEST	50213	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:20.685486078 CEST	53	50213	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:21.696197987 CEST	61793	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:21.717863083 CEST	53	61793	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:22.865897894 CEST	51699	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:22.973720074 CEST	53	51699	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:22.975537062 CEST	51185	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:22.995135069 CEST	53	51185	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:22.996891022 CEST	59594	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:23.260404110 CEST	53	59594	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:24.274667025 CEST	55591	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:24.294061899 CEST	53	55591	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:25.442476988 CEST	54646	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:25.462004900 CEST	53	54646	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:25.464106083 CEST	62070	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:25.483431101 CEST	53	62070	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:25.485399008 CEST	62243	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:25.728574991 CEST	53	62243	8.8.8.8	192.168.2.6
Jun 26, 2022 09:47:26.744364023 CEST	63198	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:47:26.764005899 CEST	53	63198	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:45:59.455624104 CEST	192.168.2.6	8.8.8.8	0x98be	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:00.972532034 CEST	192.168.2.6	8.8.8.8	0x629e	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:01.302423000 CEST	192.168.2.6	8.8.8.8	0x8c38	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:01.692954063 CEST	192.168.2.6	8.8.8.8	0xfc5b	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:03.387541056 CEST	192.168.2.6	8.8.8.8	0x96b2	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:04.861490011 CEST	192.168.2.6	8.8.8.8	0xad3d	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:05.263015985 CEST	192.168.2.6	8.8.8.8	0xb7e9	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:05.412870884 CEST	192.168.2.6	8.8.8.8	0x1817	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:06.900013924 CEST	192.168.2.6	8.8.8.8	0x8ef1	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:08.484833956 CEST	192.168.2.6	8.8.8.8	0xb4d	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:08.830322981 CEST	192.168.2.6	8.8.8.8	0x6dc3	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:09.172702074 CEST	192.168.2.6	8.8.8.8	0x3ad1	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:10.499820948 CEST	192.168.2.6	8.8.8.8	0x4e28	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:12.819227934 CEST	192.168.2.6	8.8.8.8	0x85c9	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:13.285218000 CEST	192.168.2.6	8.8.8.8	0x2bbe	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:13.464816093 CEST	192.168.2.6	8.8.8.8	0x2d75	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:14.922063112 CEST	192.168.2.6	8.8.8.8	0x15d6	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:16.272790909 CEST	192.168.2.6	8.8.8.8	0x3d72	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:16.648164988 CEST	192.168.2.6	8.8.8.8	0x2cf7	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:16.694027901 CEST	192.168.2.6	8.8.8.8	0x287e	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:18.078138113 CEST	192.168.2.6	8.8.8.8	0x7860	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:19.661204100 CEST	192.168.2.6	8.8.8.8	0x877b	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:19.972764015 CEST	192.168.2.6	8.8.8.8	0xef63	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:20.527023077 CEST	192.168.2.6	8.8.8.8	0xf017	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:21.836281061 CEST	192.168.2.6	8.8.8.8	0xb0c3	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:23.232126951 CEST	192.168.2.6	8.8.8.8	0xc28c	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:23.258554935 CEST	192.168.2.6	8.8.8.8	0xc296	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:23.283349037 CEST	192.168.2.6	8.8.8.8	0x5a53	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:24.919173002 CEST	192.168.2.6	8.8.8.8	0xb170	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:26.186084986 CEST	192.168.2.6	8.8.8.8	0x1c99	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:26.214508057 CEST	192.168.2.6	8.8.8.8	0x86e5	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:26.238574028 CEST	192.168.2.6	8.8.8.8	0xcd3	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:27.820296049 CEST	192.168.2.6	8.8.8.8	0x62cc	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:29.162329912 CEST	192.168.2.6	8.8.8.8	0x1261	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:46:29.200381994 CEST	192.168.2.6	8.8.8.8	0xc2c3	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:29.253309011 CEST	192.168.2.6	8.8.8.8	0x35a9	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:31.247152090 CEST	192.168.2.6	8.8.8.8	0xa0ee	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:32.667778969 CEST	192.168.2.6	8.8.8.8	0xa139	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:33.015280008 CEST	192.168.2.6	8.8.8.8	0x5df0	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:33.043329000 CEST	192.168.2.6	8.8.8.8	0x8bc1	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:34.348625898 CEST	192.168.2.6	8.8.8.8	0x944e	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:35.806056023 CEST	192.168.2.6	8.8.8.8	0x7aaa	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:35.834036112 CEST	192.168.2.6	8.8.8.8	0xafcb	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:35.862826109 CEST	192.168.2.6	8.8.8.8	0x1721	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:37.149254084 CEST	192.168.2.6	8.8.8.8	0x8619	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:38.397241116 CEST	192.168.2.6	8.8.8.8	0x2497	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:38.421745062 CEST	192.168.2.6	8.8.8.8	0x118d	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:38.943577051 CEST	192.168.2.6	8.8.8.8	0x2387	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:40.389466047 CEST	192.168.2.6	8.8.8.8	0x7593	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:41.557739019 CEST	192.168.2.6	8.8.8.8	0xd5ea	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:41.592691898 CEST	192.168.2.6	8.8.8.8	0xe5dd	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:41.707015991 CEST	192.168.2.6	8.8.8.8	0x240d	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:43.057265997 CEST	192.168.2.6	8.8.8.8	0x9ca0	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:44.241111040 CEST	192.168.2.6	8.8.8.8	0x9c48	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:44.268326998 CEST	192.168.2.6	8.8.8.8	0x3757	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:44.291924953 CEST	192.168.2.6	8.8.8.8	0x53dd	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:45.588435888 CEST	192.168.2.6	8.8.8.8	0x2ff2	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:46.926189899 CEST	192.168.2.6	8.8.8.8	0x6ffb	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:46.956815958 CEST	192.168.2.6	8.8.8.8	0x23cd	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:47.045470953 CEST	192.168.2.6	8.8.8.8	0x4316	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:48.388694048 CEST	192.168.2.6	8.8.8.8	0x97c2	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:49.737145901 CEST	192.168.2.6	8.8.8.8	0xdb06	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:49.759732962 CEST	192.168.2.6	8.8.8.8	0x74d5	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:49.780446053 CEST	192.168.2.6	8.8.8.8	0x30f5	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:51.131019115 CEST	192.168.2.6	8.8.8.8	0x9b03	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:52.489573956 CEST	192.168.2.6	8.8.8.8	0x6a72	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:52.512449980 CEST	192.168.2.6	8.8.8.8	0x88fa	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:52.536928892 CEST	192.168.2.6	8.8.8.8	0x4f30	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:53.803354025 CEST	192.168.2.6	8.8.8.8	0xf1b8	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:46:54.972790003 CEST	192.168.2.6	8.8.8.8	0xa4b6	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:54.994334936 CEST	192.168.2.6	8.8.8.8	0x3a03	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:55.015356064 CEST	192.168.2.6	8.8.8.8	0xe6d2	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:56.287367105 CEST	192.168.2.6	8.8.8.8	0x3ba8	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:57.506583929 CEST	192.168.2.6	8.8.8.8	0x8265	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:57.533893108 CEST	192.168.2.6	8.8.8.8	0x4e6d	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:57.560184956 CEST	192.168.2.6	8.8.8.8	0xa2a0	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:58.850754976 CEST	192.168.2.6	8.8.8.8	0x69ca	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:00.019772053 CEST	192.168.2.6	8.8.8.8	0xef71	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:00.040926933 CEST	192.168.2.6	8.8.8.8	0x54f	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:00.064255953 CEST	192.168.2.6	8.8.8.8	0x8b9	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:01.320076942 CEST	192.168.2.6	8.8.8.8	0x2232	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:02.488662004 CEST	192.168.2.6	8.8.8.8	0xf642	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:02.834417105 CEST	192.168.2.6	8.8.8.8	0xe751	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:02.855746984 CEST	192.168.2.6	8.8.8.8	0x878c	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:04.116741896 CEST	192.168.2.6	8.8.8.8	0x9625	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:05.284356117 CEST	192.168.2.6	8.8.8.8	0x196a	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:05.593838930 CEST	192.168.2.6	8.8.8.8	0x5033	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:06.250915051 CEST	192.168.2.6	8.8.8.8	0x9f4e	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:07.654623985 CEST	192.168.2.6	8.8.8.8	0x74ca	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:08.926732063 CEST	192.168.2.6	8.8.8.8	0xd8f7	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:09.218846083 CEST	192.168.2.6	8.8.8.8	0xed77	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:09.238074064 CEST	192.168.2.6	8.8.8.8	0x8f1	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:10.585858107 CEST	192.168.2.6	8.8.8.8	0xbd0e	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:11.740303040 CEST	192.168.2.6	8.8.8.8	0x4e35	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:12.144227982 CEST	192.168.2.6	8.8.8.8	0xe8fa	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:12.167809010 CEST	192.168.2.6	8.8.8.8	0xbac1	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:13.602176905 CEST	192.168.2.6	8.8.8.8	0xad50	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:14.769234896 CEST	192.168.2.6	8.8.8.8	0xd077	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:14.792699099 CEST	192.168.2.6	8.8.8.8	0xfd7c	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:15.100631952 CEST	192.168.2.6	8.8.8.8	0x54e4	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:16.445960999 CEST	192.168.2.6	8.8.8.8	0xcfd7	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:17.613542080 CEST	192.168.2.6	8.8.8.8	0xf6a9	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:17.632636070 CEST	192.168.2.6	8.8.8.8	0xcfc1	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:17.922254086 CEST	192.168.2.6	8.8.8.8	0xc18	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:47:19.196216106 CEST	192.168.2.6	8.8.8.8	0x5d04	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:20.366450071 CEST	192.168.2.6	8.8.8.8	0x951d	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:20.390060902 CEST	192.168.2.6	8.8.8.8	0xad41	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:20.413465977 CEST	192.168.2.6	8.8.8.8	0x8a5b	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:21.696197987 CEST	192.168.2.6	8.8.8.8	0x549b	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:22.865897894 CEST	192.168.2.6	8.8.8.8	0x72df	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:22.975537062 CEST	192.168.2.6	8.8.8.8	0x123	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:22.996891022 CEST	192.168.2.6	8.8.8.8	0x5478	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:24.274667025 CEST	192.168.2.6	8.8.8.8	0xdd42	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:25.442476988 CEST	192.168.2.6	8.8.8.8	0xc3ae	Standard query (0)	kalskala.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:25.464106083 CEST	192.168.2.6	8.8.8.8	0x699f	Standard query (0)	tuekisaa.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:25.485399008 CEST	192.168.2.6	8.8.8.8	0xf0de	Standard query (0)	parthaha.ac.ug	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:26.744364023 CEST	192.168.2.6	8.8.8.8	0x28d	Standard query (0)	nikahuve.ac.ug	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:45:59.609529972 CEST	8.8.8.8	192.168.2.6	0x98be	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:01.287909031 CEST	8.8.8.8	192.168.2.6	0x629e	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:01.668832064 CEST	8.8.8.8	192.168.2.6	0x8c38	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:02.335402966 CEST	8.8.8.8	192.168.2.6	0xfc5b	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:03.521174908 CEST	8.8.8.8	192.168.2.6	0x96b2	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:05.224469900 CEST	8.8.8.8	192.168.2.6	0xad3d	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:05.407883883 CEST	8.8.8.8	192.168.2.6	0xb7e9	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:05.879934072 CEST	8.8.8.8	192.168.2.6	0x1817	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:07.183330059 CEST	8.8.8.8	192.168.2.6	0x8ef1	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:08.825110912 CEST	8.8.8.8	192.168.2.6	0xb4d	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:09.151824951 CEST	8.8.8.8	192.168.2.6	0x6dc3	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:09.415802002 CEST	8.8.8.8	192.168.2.6	0x3ad1	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:10.522844076 CEST	8.8.8.8	192.168.2.6	0x4e28	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:13.254749060 CEST	8.8.8.8	192.168.2.6	0x85c9	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:13.417113066 CEST	8.8.8.8	192.168.2.6	0x2bbe	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:13.861335993 CEST	8.8.8.8	192.168.2.6	0x2d75	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:14.943308115 CEST	8.8.8.8	192.168.2.6	0x15d6	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:16.600392103 CEST	8.8.8.8	192.168.2.6	0x3d72	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:16.668729067 CEST	8.8.8.8	192.168.2.6	0x2cf7	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:17.050290108 CEST	8.8.8.8	192.168.2.6	0x287e	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)

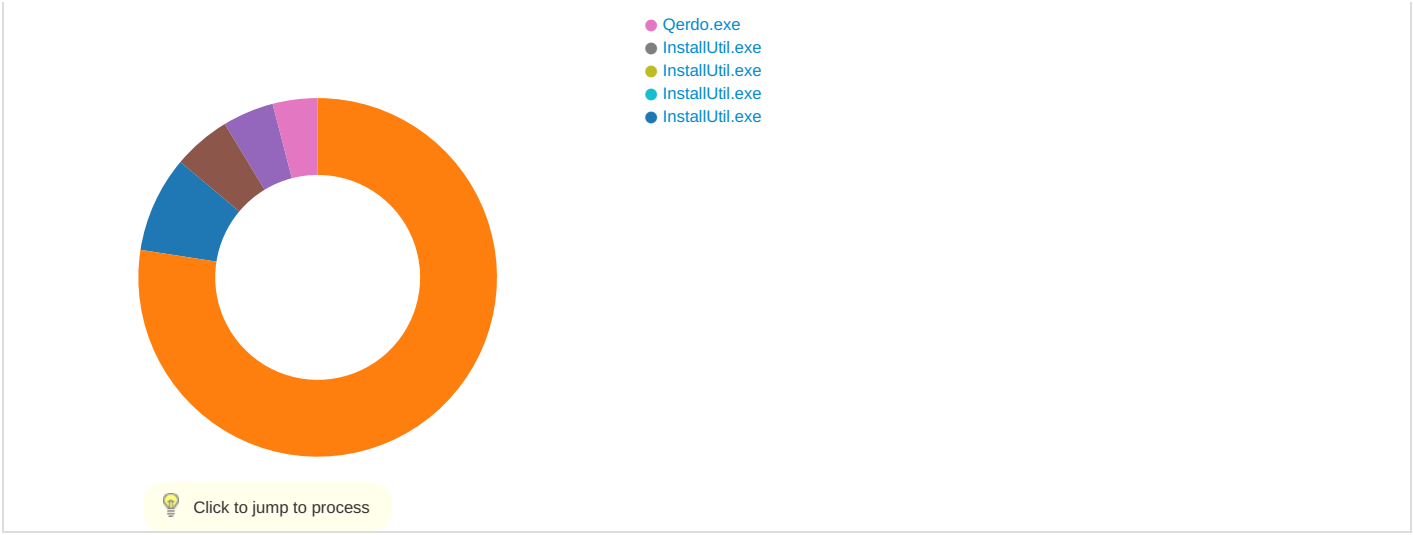
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:46:18.172508955 CEST	8.8.8.8	192.168.2.6	0x7860	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:19.946038008 CEST	8.8.8.8	192.168.2.6	0x877b	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:20.489490032 CEST	8.8.8.8	192.168.2.6	0xef63	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:20.808574915 CEST	8.8.8.8	192.168.2.6	0xf017	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:21.855746031 CEST	8.8.8.8	192.168.2.6	0xb0c3	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:23.251566887 CEST	8.8.8.8	192.168.2.6	0xc28c	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:23.277683020 CEST	8.8.8.8	192.168.2.6	0xc296	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:23.900996923 CEST	8.8.8.8	192.168.2.6	0x5a53	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:24.938805103 CEST	8.8.8.8	192.168.2.6	0xb170	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:26.206334114 CEST	8.8.8.8	192.168.2.6	0x1c99	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:26.233730078 CEST	8.8.8.8	192.168.2.6	0x86e5	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:26.787453890 CEST	8.8.8.8	192.168.2.6	0xcd3	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:27.842549086 CEST	8.8.8.8	192.168.2.6	0x62cc	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:29.182220936 CEST	8.8.8.8	192.168.2.6	0x1261	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:29.220069885 CEST	8.8.8.8	192.168.2.6	0xc2c3	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:29.535430908 CEST	8.8.8.8	192.168.2.6	0x35a9	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:31.267640114 CEST	8.8.8.8	192.168.2.6	0xa0ee	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:33.007348061 CEST	8.8.8.8	192.168.2.6	0xa139	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:33.037226915 CEST	8.8.8.8	192.168.2.6	0x5df0	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:33.318209887 CEST	8.8.8.8	192.168.2.6	0x8bc1	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:34.429868937 CEST	8.8.8.8	192.168.2.6	0x944e	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:35.827079058 CEST	8.8.8.8	192.168.2.6	0x7aaa	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:35.855199099 CEST	8.8.8.8	192.168.2.6	0xafcb	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:36.128879070 CEST	8.8.8.8	192.168.2.6	0x1721	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:37.234436989 CEST	8.8.8.8	192.168.2.6	0x8619	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:38.417606115 CEST	8.8.8.8	192.168.2.6	0x2497	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:38.926244020 CEST	8.8.8.8	192.168.2.6	0x118d	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:39.367716074 CEST	8.8.8.8	192.168.2.6	0x2387	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:40.409852028 CEST	8.8.8.8	192.168.2.6	0x7593	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:41.579132080 CEST	8.8.8.8	192.168.2.6	0xd5ea	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:41.702279091 CEST	8.8.8.8	192.168.2.6	0xe5dd	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:42.044704914 CEST	8.8.8.8	192.168.2.6	0x240d	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:43.077081919 CEST	8.8.8.8	192.168.2.6	0x9ca0	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:44.260705948 CEST	8.8.8.8	192.168.2.6	0x9c48	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:44.287756920 CEST	8.8.8.8	192.168.2.6	0x3757	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:46:44.559916019 CEST	8.8.8.8	192.168.2.6	0x53dd	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:45.608629942 CEST	8.8.8.8	192.168.2.6	0x2ff2	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:46.948671103 CEST	8.8.8.8	192.168.2.6	0x6ffb	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:46.984714985 CEST	8.8.8.8	192.168.2.6	0x23cd	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:47.373270035 CEST	8.8.8.8	192.168.2.6	0x4316	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:48.407943964 CEST	8.8.8.8	192.168.2.6	0x97c2	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:49.756731033 CEST	8.8.8.8	192.168.2.6	0xdb06	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:49.778947115 CEST	8.8.8.8	192.168.2.6	0x74d5	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:50.115060091 CEST	8.8.8.8	192.168.2.6	0x30f5	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:51.151547909 CEST	8.8.8.8	192.168.2.6	0x9b03	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:52.510042906 CEST	8.8.8.8	192.168.2.6	0x6a72	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:52.535131931 CEST	8.8.8.8	192.168.2.6	0x88fa	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:52.786977053 CEST	8.8.8.8	192.168.2.6	0x4f30	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:53.820684910 CEST	8.8.8.8	192.168.2.6	0xf1b8	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:54.992006063 CEST	8.8.8.8	192.168.2.6	0xa4b6	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:55.012367964 CEST	8.8.8.8	192.168.2.6	0x3a03	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:55.273374081 CEST	8.8.8.8	192.168.2.6	0xe6d2	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:56.363706112 CEST	8.8.8.8	192.168.2.6	0x3ba8	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:57.528808117 CEST	8.8.8.8	192.168.2.6	0x8265	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:57.558281898 CEST	8.8.8.8	192.168.2.6	0x4e6d	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:57.833945036 CEST	8.8.8.8	192.168.2.6	0xa2a0	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:46:58.872860909 CEST	8.8.8.8	192.168.2.6	0x69ca	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:00.037149906 CEST	8.8.8.8	192.168.2.6	0xef71	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:00.062521935 CEST	8.8.8.8	192.168.2.6	0x54f	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:00.309726000 CEST	8.8.8.8	192.168.2.6	0x8b9	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:01.341156960 CEST	8.8.8.8	192.168.2.6	0x2232	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:02.832598925 CEST	8.8.8.8	192.168.2.6	0xf642	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:02.853538036 CEST	8.8.8.8	192.168.2.6	0xe751	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:03.110609055 CEST	8.8.8.8	192.168.2.6	0x878c	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:04.133922100 CEST	8.8.8.8	192.168.2.6	0x9625	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:05.592148066 CEST	8.8.8.8	192.168.2.6	0x196a	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:05.879611015 CEST	8.8.8.8	192.168.2.6	0x5033	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:06.517442942 CEST	8.8.8.8	192.168.2.6	0x9f4e	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:07.788269043 CEST	8.8.8.8	192.168.2.6	0x74ca	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:09.216793060 CEST	8.8.8.8	192.168.2.6	0xd8f7	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:47:09.236004114 CEST	8.8.8.8	192.168.2.6	0xed77	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:09.571846008 CEST	8.8.8.8	192.168.2.6	0x8f1	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:10.603106976 CEST	8.8.8.8	192.168.2.6	0xbd0e	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:12.141793966 CEST	8.8.8.8	192.168.2.6	0x4e35	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:12.163436890 CEST	8.8.8.8	192.168.2.6	0xe8fa	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:12.589550972 CEST	8.8.8.8	192.168.2.6	0xbac1	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:13.621402979 CEST	8.8.8.8	192.168.2.6	0xad50	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:14.788824081 CEST	8.8.8.8	192.168.2.6	0xd077	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:15.098356962 CEST	8.8.8.8	192.168.2.6	0xfd7c	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:15.432835102 CEST	8.8.8.8	192.168.2.6	0x54e4	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:16.467267990 CEST	8.8.8.8	192.168.2.6	0xcfd7	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:17.630446911 CEST	8.8.8.8	192.168.2.6	0xf6a9	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:17.920314074 CEST	8.8.8.8	192.168.2.6	0xcfc1	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:18.181885004 CEST	8.8.8.8	192.168.2.6	0xc18	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:19.217360020 CEST	8.8.8.8	192.168.2.6	0x5d04	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:20.387876034 CEST	8.8.8.8	192.168.2.6	0x951d	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:20.411376953 CEST	8.8.8.8	192.168.2.6	0xad41	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:20.685486078 CEST	8.8.8.8	192.168.2.6	0x8a5b	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:21.717863083 CEST	8.8.8.8	192.168.2.6	0x549b	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:22.973720074 CEST	8.8.8.8	192.168.2.6	0x72df	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:22.995135069 CEST	8.8.8.8	192.168.2.6	0x123	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:23.260404110 CEST	8.8.8.8	192.168.2.6	0x5478	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:24.294061899 CEST	8.8.8.8	192.168.2.6	0xdd42	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:25.462004900 CEST	8.8.8.8	192.168.2.6	0xc3ae	Name error (3)	kalskala.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:25.483431101 CEST	8.8.8.8	192.168.2.6	0x699f	Name error (3)	tuekisaa.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:25.728574991 CEST	8.8.8.8	192.168.2.6	0xf0de	Server failure (2)	parthaha.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:47:26.764005899 CEST	8.8.8.8	192.168.2.6	0x28d	No error (0)	nikahuve.ac.ug		194.5.98.107	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: kyFBQxVbsg.exe PID: 6232, Parent PID: 752

General

Target ID:	0
Start time:	09:44:41
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\kyFBQxVbsg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\kyFBQxVbsg.exe"
Imagebase:	0x2e0000
File size:	735232 bytes
MD5 hash:	972334F0C55D0AEAB0B32EFE41EA3470
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.526374372.0000000003850000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.540068634.000000000269C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.541310066.000000000382F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.541870137.0000000004BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.541870137.0000000004BA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.541421315.00000000038CF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ppjollp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA0BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6DA2EAF6	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6DA2EAF6	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kyFBQxVbsg.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DECC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 23 1a fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0a 00 00 46 00 00 00 00 00 00 fd 0e 0b 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 0b 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL#b0F @ `	success or wait	3	6DA2EAF6	unknown
C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6DA2EAF6	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kyFBQxVbsg.exe.log	0	805	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DECC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAF03DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Qerdo	unicode	"C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe"	success or wait	1	6CA0646A	RegSetValueExW

Analysis Process: powershell.exe PID: **6288**, Parent PID: **6232**

General

Target ID:	3
Start time:	09:44:48
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMQAwADsAIABTAGUAdAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAGEAdABoACAAJwBDADoAXAAnAA==
Imagebase:	0xf10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBBCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_esjq1xkt.ffx.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CA01E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pshfc5wv.vht.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CA01E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220626	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA0BEFF	CreateDirectoryW
C:\Users\user\Documents\20220626\PowerShell_transcript.128757.EFYe5VSb.20220626094450.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CA01E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_esjq1xkt.ffx.ps1	success or wait	1	6CA06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pshfc5wv.vht.psm1	success or wait	1	6CA06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_esjq1xkt.ffx.ps1	0	1	31	1	success or wait	1	6CA01B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pshfc5wv.vht.psm1	0	1	31	1	success or wait	1	6CA01B4F	WriteFile
C:\Users\user\Documents\20220626\PowerShell_transcript.128757.EFYe5VSb.20220626094450.txt	0	3	ff		success or wait	1	6CA01B4F	WriteFile
C:\Users\user\Documents\20220626\PowerShell_transcript.128757.EFYe5VSb.20220626094450.txt	3	779	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 36 32 36 30 39 34 35 30 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 38 37 35 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220626094508Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 128757 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	44	6CA01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 fd 23 79 3b 9f fd 08 51 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 73 54 72 61 6e 73 66 65 72 5c 42 69 74 73 54 72 61 6e 73 66 65 72 2e 70 73 64 31 08 00 00 00 12 00 00 00 53 74 61 72 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 53 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 47 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 13 00 00 00 52 65 73 75 6d 65 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 0c 00 00 00 41 64 64 2d 42 69 74 73 46 69 6c 65 08 00 00 00 14 00 00 00 53 75 73 70 65 6e 64 2d 42 69 74 73 54 72 61	PSMODULECACHE#y;QC:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1Start-BitsTransferSet-BitsTransferGet-BitsTransferResume-BitsTransferAdd-BitsFileSuspend-BitsTra	success or wait	1	6CA01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 4c 6f 63 6b 65 72 5c 42 69 74 4c 6f 63 6b 65 72 2e 70 73 6d 31 28 00 00 00 20 00 00 00 41 64 64 2d 45 78 74 65 72 6e 61 6c 4b 65 79 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 19 00 00 00 43 6c 65 61 72 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 44 69 73 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 47 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1b 00 00 00 53 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 45 6e 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74	wsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1(Add-ExternalKeyProtectorInternalClear-BitLockerAutoUnlockDisable-BitLockerAutoUnlockGet-BitLockerVolumeInternalSet-BitLockerVolumeInternalEnable-BitLockerAut	success or wait	1	6CA01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	72 64 08 00 00 00 0d 00 00 00 53 74 61 72 74 2d 50 72 6f 63 65 73 73 08 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 49 74 65 6d 08 00 00 00 0d 00 00 00 53 74 6f 70 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 09 00 00 00 4a 6f 69 6e 2d 50 61 74 68 08 00 00 00 0c 00 00 00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 1a 00 00 00 54 65 73 74 2d 43 6f 6d 70 75 74 65 72 53 65 63 75 72 65 43 68 61 6e 6e 65 6c 08 00 00 00 0e 00 00 00 4c 69 6d 69 74 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 10 00 00 00 49 6e 76 6f 6b 65 2d 57 6d 69 4d 65 74 68 6f 64 08 00 00 00 10 00 00 00 47 65 74 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0b 00 00 00 4e 65	rdStart-ProcessInvoke-ItemStop-ComputerGet-HotFixJoin-PathStop-ProcessTest-ComputerSecureChannelLimit-EventLogInvoke-WmiMethodGet-ItemPropertyRemove-ComputerNe	success or wait	1	6CA01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	12288	2446	3b 9f fd 08 71 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 08 00 00 00 47 65 74 2d 44 61 74 65 08 00 00 00 0e 00 00 00 43 6c 65 61 72 2d 56 61 72 69 61 62 6c 65 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 0a 00 00 00 49 6d 70 6f 72 74 2d 43 73 76 08 00 00 00 0c 00 00 00 47 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0c 00 00 00 4e 65 77 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f	;qC:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mGet-DateClear-VariableGet-EventSubscriberImport-CsvGet-VariableNew-VariableCo	success or wait	1	6CA01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 60 14 00 00 19 00 00 00 fd 0b fd 04 3e 07 33 07 30 07 00 00 00 00 fd 00 0d 00 fd 0b 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e`>30@	success or wait	1	6DE876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 3a 00 00 00 0e 00 20 00	H<@^L"My::	success or wait	17	6DE876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DE876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DE876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DE876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 09 06 fd 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 16 3b 40 01 fd 44 40 01 40 4d 40 01 3c 4d 00 01 24 4d 00 01 1b 3b 40 01 38 4d 00 01 3f 4d 00 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@Xd@Vd@*@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@;@D@@M@<M$M;@8M?M;@<@<@<@W@M@	success or wait	11	6DE876FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB95705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DBA1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DBA203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAF03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CA01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CA01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	67	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CA01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CA01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CA01B4F	ReadFile

Analysis Process: conhost.exe PID: **6424**, Parent PID: **6288**

General

Target ID:	5
Start time:	09:44:49
Start date:	26/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: InstallUtil.exe PID: **2328**, Parent PID: **6232**

General

Target ID:	16
Start time:	09:45:54
Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x60000
File size:	41064 bytes

MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: InstallUtil.exe PID: **6528**, Parent PID: **6232**

General

Target ID:	17
Start time:	09:45:55
Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xae0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.535499326.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000000.535499326.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000000.535499326.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.533973605.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000000.533973605.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000000.533973605.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.536706156.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000000.536706156.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000000.536706156.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.533640248.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000000.533640248.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000000.533640248.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.534323754.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000000.534323754.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000000.534323754.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000002.645272430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000002.645272430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000002.645272430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.536064780.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000000.536064780.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000000.536064780.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.534848870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000011.00000000.534848870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000011.00000000.534848870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000002.646242553.00000000011E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\forbas	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	408EAC	CreateDirectoryW
C:\Users\user\AppData\Roaming\forbas\scxs.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	418956	CreateFileW
C:\Users\user\AppData\Roaming\forbas	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408EAC	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\forbas\scxs.dat	0	192	fd 6a fd 56 fd 4a fd fd 21 6b 55 5f fd 02 73 59 fd 5b 17 74 fd fd 07 17 07 7c 5d fd fd 25 89 fd fd 2a 21 fd 41 5d 08 79 2a fd 78 04 fd fd 1a fd fd 4c fd 42 fd 1e 25 fd fd fd 43 fd fd fd fd fd fd 3d 26 66 26 fd fd 56 6e fd 7d fd fd fd 24 fd 50 fd fd fd fd 7b 6a 2e 67 6c fd fd fd fd fd fd 1a 4e 69 3a fd 6f fd 73 fd 2f 1c 3d a9 1f fd 66 4c fd fd 03 63 16 07 3c fd 41 fd fd 56 31 fd fd fd 34 58 3e fd 22 fd 7c fd 60 fd fd fd f0 43 fd fd 6d 37 5b 75 fd 1b fd 1c 24 46 27 29 35 fd fd 64 04 fd 70 3b 18 fd fd fd 32 16 fd fd 1a 4d 42 fd 24 fd ff 2d fd	jVJ!kU_sY[t|]%*!A]yxLBC=&f&Vn}$P{j.glNi:os/=fLc<AV14X>"\|`Cm7[u$F')5dp;2MB$-	success or wait	2	418990	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\forbas\scxs.dat	unknown	192	success or wait	1	4189FD	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\cvxyttydfsgbghfgfhtd-RXTSAM\	success or wait	1	410CF7	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\cvxyttydfsgbghfgfhtd-RXTSAM	exepath	binary	D0 6A 9D 56 D1 4A DD E6 78 6B 09 5F FC 02 33 59 9E 5B 52 74 EF D5 A7 87 48 07 3F 5D DF FC 73 C2 C0 EE AC 2A 72 99 0F 5D 13 79 BA AA E7 78 1F EE C9 1A A1 FE 52 B4 4A 90 1D CC A5 E0 D1 A2 67 F7 FF 8F D1 F6 A8 A3 DE 3D 75 66 6F EB A3 56 32 AC 6E A7 D5 A3 63 E9 00 82 E0 A0 DD 7B 46 2E 6D 6C 87 C1 FA E8 A6 D1 7B 4E 0F 3A B5 6F 8E 73 D2 2F 1E 3D AD A9 77 F7 14 4C C0 DE 09 63	success or wait	1	410D1F	RegSetValueExA
HKEY_CURRENT_USER\Software\cvxyttydfsgbghfgfhtd-RXTSAM	licence	unicode	8398D86D5E1B03A50DF13C3DEECDF12F	success or wait	1	410D1F	RegSetValueExA

Analysis Process: Qerdo.exe PID: **6216**, Parent PID: **3688**

General

Target ID:	19

Start time:	09:46:02
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe"
Imagebase:	0x40000
File size:	735232 bytes
MD5 hash:	972334F0C55D0AEAB0B32EFE41EA3470
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000013.00000002.597952189.000000000239C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000013.00000002.606363285.00000000048F0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000013.00000002.606363285.00000000048F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000013.00000002.603389337.000000000352F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000013.00000003.581326592.0000000003550000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000013.00000002.605837275.00000000035CF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 58%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Qerdo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DECC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Qerdo.exe.log	0	805	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DECC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAF03DE	ReadFile

Analysis Process: Qerdo.exe PID: **5652**, Parent PID: **3688**

General

Target ID:	24
Start time:	09:46:12
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Ppjollp\Qerdo.exe"
Imagebase:	0x9a0000
File size:	735232 bytes
MD5 hash:	972334F0C55D0AEAB0B32EFE41EA3470
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000018.00000002.612287399.00000000040DF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000018.00000003.587908821.0000000004060000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000018.00000002.610776047.0000000002EAC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000018.00000002.612156985.000000000403F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000018.00000002.613026227.0000000005440000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000018.00000002.613026227.0000000005440000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAF03DE	ReadFile

Analysis Process: InstallUtil.exe PID: **2592**, Parent PID: **6216**

General

Target ID:	25
Start time:	09:46:20
Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xe0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: InstallUtil.exe PID: **5836**, Parent PID: **6216**

General

Target ID:	26
Start time:	09:46:22
Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x5d0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000000.594041394.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000000.594041394.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000000.594041394.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000000.592527384.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000000.592527384.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000000.592527384.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000000.591921739.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000000.591921739.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000000.591921739.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000000.593660616.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000000.593660616.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000000.593660616.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000000.594464654.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000000.594464654.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000000.594464654.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000000.595033873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000000.595033873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000000.595033873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000002.596165958.0000000000BC7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000000.593157225.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000000.593157225.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000000.593157225.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000002.595851570.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001A.00000002.595851570.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000002.595851570.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	high

Analysis Process: InstallUtil.exe PID: **4900**, Parent PID: **5652**

General	
Target ID:	27
Start time:	09:46:23
Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x260000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: InstallUtil.exe PID: **6304**, Parent PID: **5652**

General	
Target ID:	28
Start time:	09:46:25

Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x510000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000000.601490372.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000000.601490372.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000000.601490372.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000002.607934228.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000002.607934228.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000002.607934228.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000000.598510412.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000000.598510412.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000000.598510412.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000000.606949507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000000.606949507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000000.606949507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000000.603526142.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000000.603526142.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000000.603526142.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000000.599641579.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000000.599641579.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000000.599641579.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000000.599125899.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000000.599125899.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000000.599125899.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000002.608522925.0000000000B37000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000000.606295959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 0000001C.00000000.606295959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001C.00000000.606295959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	high

Disassembly

No disassembly