Analysis of some...
PEGASUS
Source Code Leak

Pegasus - Zero Click Spyware - NSO

Pegasus – Remote Administration Tool

Cyber espionage tools

Content created by

Alexandru Angheluș | Oana Buzianu | Aris Giannopoulos

www.prodefence.ro | contact@prodefence.ro

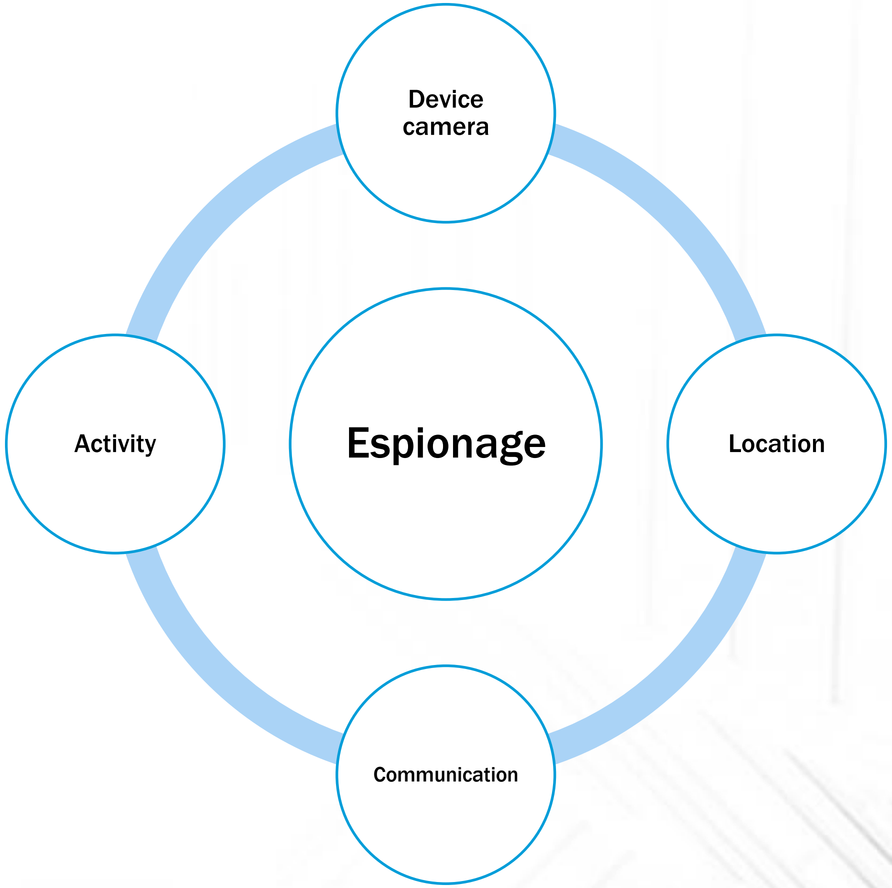
ProDefence
Cyber Security Services

A source code - an opportunity to find out the secrets of malware applications

- Pegasus – Zero Click Spyware
- Pegasus – Remote Administration Tool
- Analysis of what the source code represents

Cyber espionage tools

- Full control of compromised devices
- Exploitation of resources and information
- Monitoring private and professional life



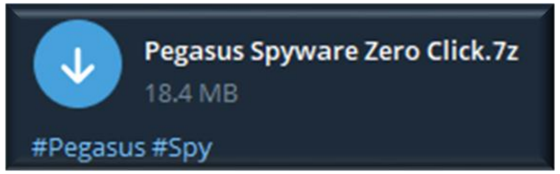
The leaked source

Starting from Telegram

Pegasus Spyware Zero Click – One of the most dangerous applications of cyber espionage. If most applications require the victim to click on something, it seems that in the case of Zero Click Spyware it is enough for the target device to receive an SMS. The device is compromised and under the control of the attacker.

The publication of the source code is an opportunity for cybersecurity specialists to discover the secrets of international cyber espionage.

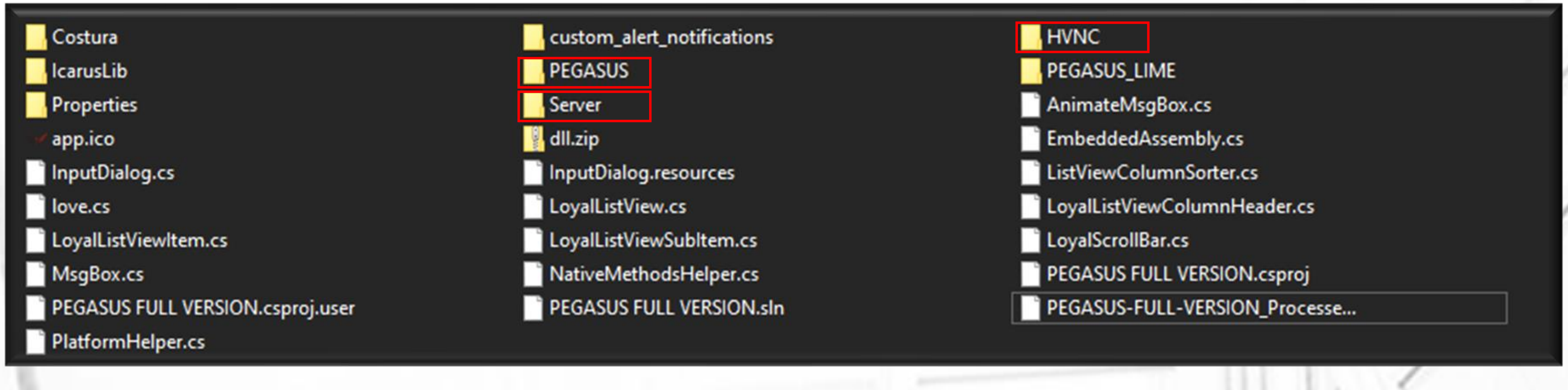
We're going to explore the files we found to see if we're really that lucky.



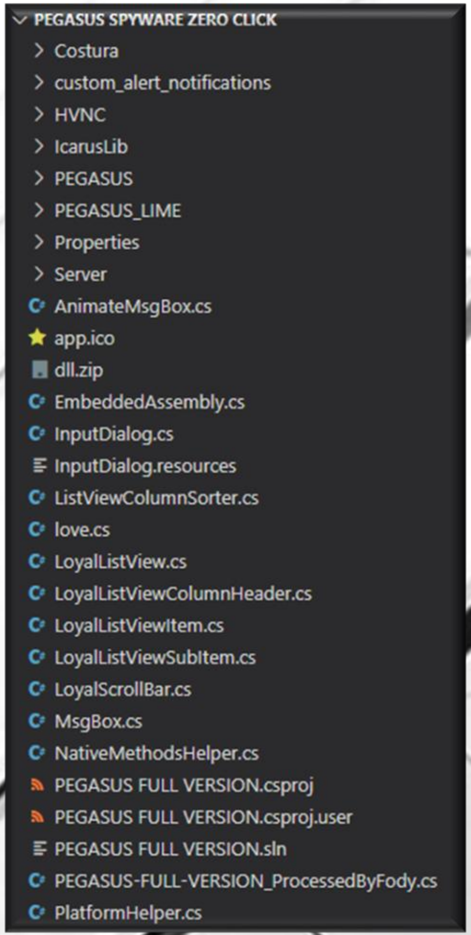
Pegasus Spyware Zero Click.7z

18.4 MB

#Pegasus #Spy



Costura
custom_alert_notifications
HVNC
IcarusLib
PEGASUS
PEGASUS_LIME
Properties
Server
AnimateMsgBox.cs
app.ico
dll.zip
EmbeddedAssembly.cs
InputDialog.cs
InputDialog.resources
ListViewColumnSorter.cs
love.cs
LoyalListView.cs
LoyalListViewColumnHeader.cs
LoyalListViewItem.cs
LoyalListViewSubItem.cs
LoyalScrollBar.cs
MsgBox.cs
NativeMethodsHelper.cs
PEGASUS FULL VERSION.csproj
PEGASUS FULL VERSION.csproj.user
PEGASUS FULL VERSION.sln
PEGASUS-FULL-VERSION_Processe...
PlatformHelper.cs



PEGASUS SPYWARE ZERO CLICK
> Costura
> custom_alert_notifications
> HVNC
> IcarusLib
> PEGASUS
> PEGASUS_LIME
> Properties
> Server
AnimateMsgBox.cs
app.ico
dll.zip
EmbeddedAssembly.cs
InputDialog.cs
InputDialog.resources
ListViewColumnSorter.cs
love.cs
LoyalListView.cs
LoyalListViewColumnHeader.cs
LoyalListViewItem.cs
LoyalListViewSubItem.cs
LoyalScrollBar.cs
MsgBox.cs
NativeMethodsHelper.cs
PEGASUS FULL VERSION.csproj
PEGASUS FULL VERSION.csproj.user
PEGASUS FULL VERSION.sln
PEGASUS-FULL-VERSION_ProcessedByFody.cs
PlatformHelper.cs

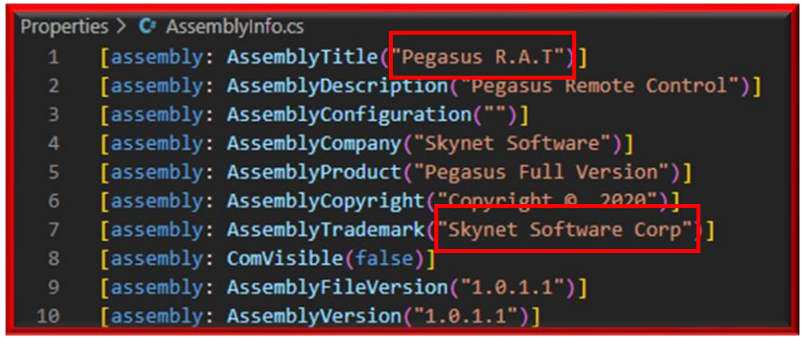
The downloaded files contain elements that indicate the existence of an interesting project and close to what we hope to be.

The presence of PEGASUS, Server, HVNC files can be considered parts of the desired spyware tool.

The leaked source

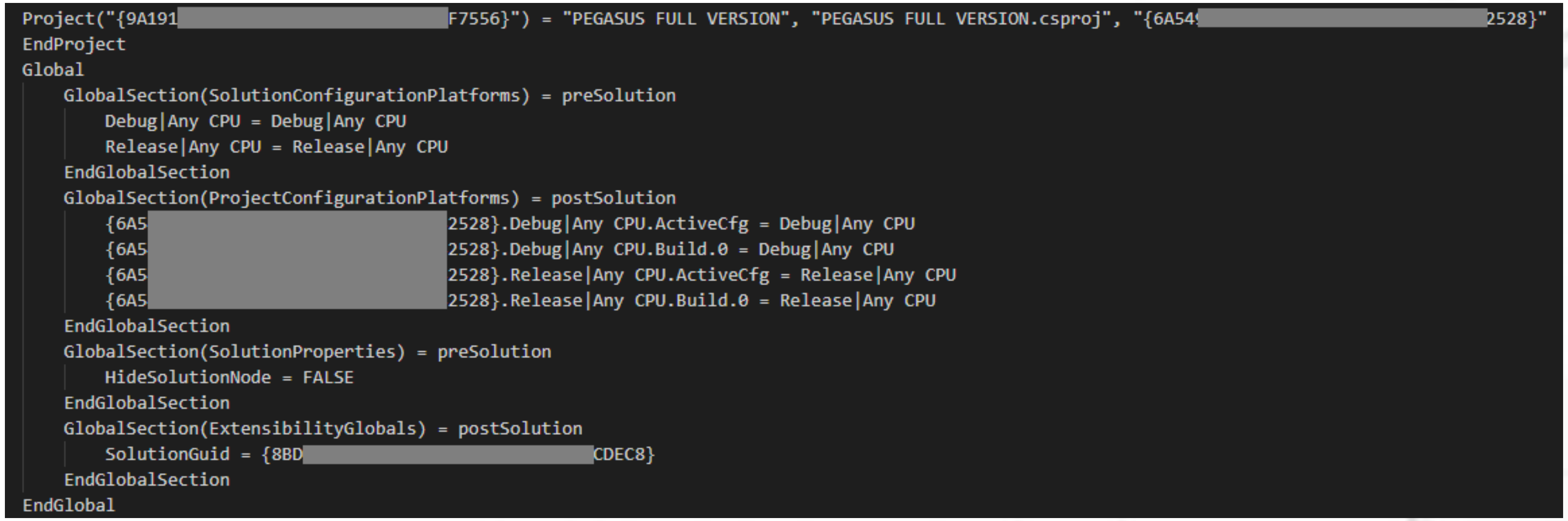
The point of disappointment

Version information, author, resources help identify the basics of the application



Properties > AssemblyInfo.cs

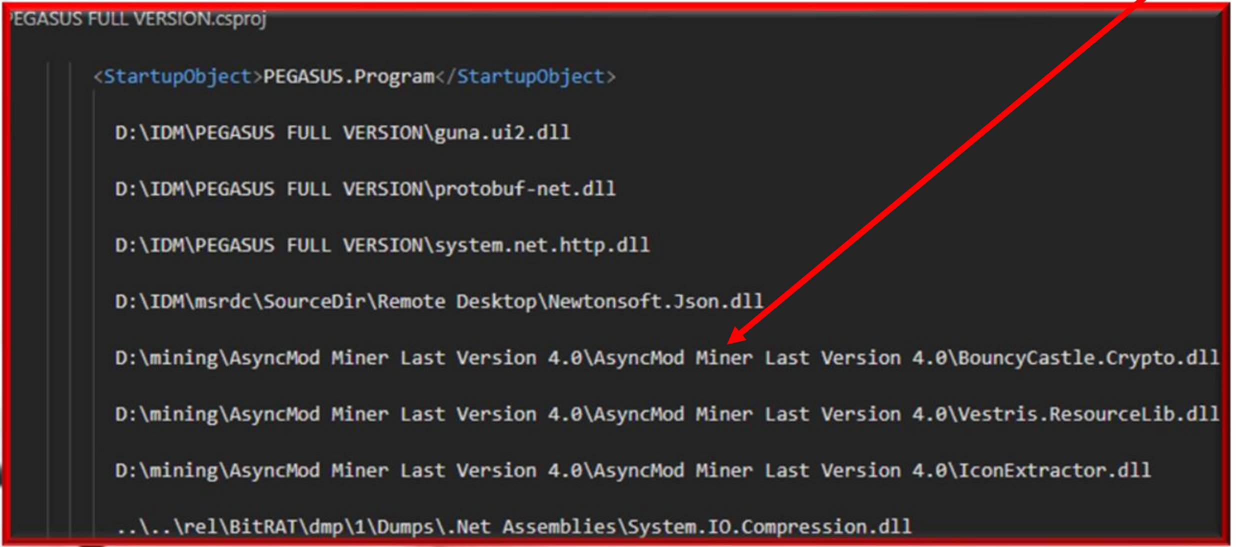
```
[assembly: AssemblyTitle("Pegasus R.A.T")]
[assembly: AssemblyDescription("Pegasus Remote Control")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("Skynet Software")]
[assembly: AssemblyProduct("Pegasus Full Version")]
[assembly: AssemblyCopyright("Copyright ©  2020")]
[assembly: AssemblyTrademark("Skynet Software Corp")]
[assembly: ComVisible(false)]
[assembly: AssemblyFileVersion("1.0.1.1")]
[assembly: AssemblyVersion("1.0.1.1")]
```



```
Project("{9A191[redacted]F7556}") = "PEGASUS FULL VERSION", "PEGASUS FULL VERSION.csproj", "{6A54[redacted]2528}"
EndProject
Global
    GlobalSection(SolutionConfigurationPlatforms) = preSolution
        Debug|Any CPU = Debug|Any CPU
        Release|Any CPU = Release|Any CPU
    EndGlobalSection
    GlobalSection(ProjectConfigurationPlatforms) = postSolution
        {6A5[redacted]2528}.Debug|Any CPU.ActiveCfg = Debug|Any CPU
        {6A5[redacted]2528}.Debug|Any CPU.Build.0 = Debug|Any CPU
        {6A5[redacted]2528}.Release|Any CPU.ActiveCfg = Release|Any CPU
        {6A5[redacted]2528}.Release|Any CPU.Build.0 = Release|Any CPU
    EndGlobalSection
    GlobalSection(SolutionProperties) = preSolution
        HideSolutionNode = FALSE
    EndGlobalSection
    GlobalSection(ExtensibilityGlobals) = postSolution
        SolutionGuid = {8BD[redacted]CDEC8}
    EndGlobalSection
EndGlobal
```

The first clue to misleading.

Pegasus Remote Control created by Skynet Software Corp – 2020.
Seems that there is no NSO Group and no Pegasus spyware source code...



'EGASUS FULL VERSION.csproj

```
    <StartupObject>PEGASUS.Program</StartupObject>

      D:\IDM\PEGASUS FULL VERSION\guna.ui2.dll

      D:\IDM\PEGASUS FULL VERSION\protobuf-net.dll

      D:\IDM\PEGASUS FULL VERSION\system.net.http.dll

      D:\IDM\msrdc\SourceDir\Remote Desktop\Newtonsoft.Json.dll

      D:\mining\AsyncMod Miner Last Version 4.0\AsyncMod Miner Last Version 4.0\BouncyCastle.Crypto.dll

      D:\mining\AsyncMod Miner Last Version 4.0\AsyncMod Miner Last Version 4.0\Vestris.ResourceLib.dll

      D:\mining\AsyncMod Miner Last Version 4.0\AsyncMod Miner Last Version 4.0\IconExtractor.dll

      ..\..\rel\BitRAT\dmp\1\Dumps\.Net Assemblies\System.IO.Compression.dll
```

The second clue

Espionage is distinguished by its silent and hidden actions.
The analyzed project contains the option to use the resources of the compromised device to mine cryptocurrencies, so the application may not be the desired one.

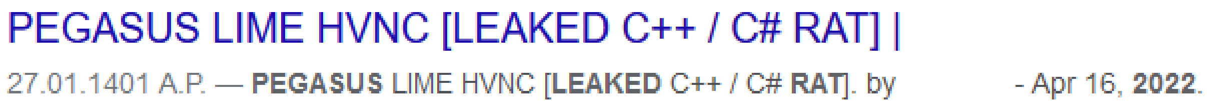
As you can see, it has its components:

- Windows remote desktop manager
- AsyncMod Miner
- BitRat (Remote Administration Tool)

The leaked source

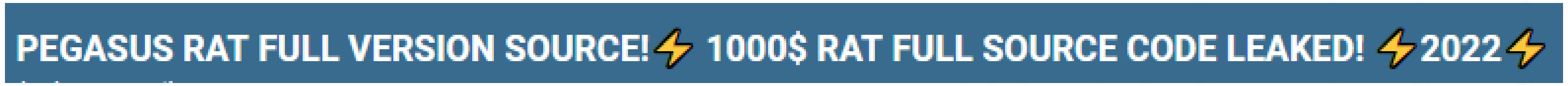
Google -> Pegasus rat leak 2022

As usually, Google can answer the right questions. It appears that the source of a Pegasus has been made public, but one developed by the NSO Group.

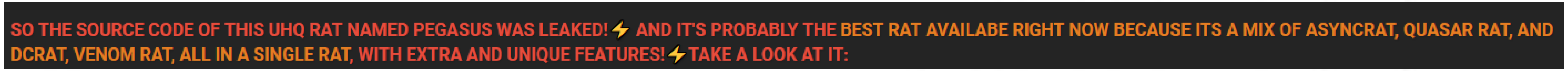


PEGASUS LIME HVNC [LEAKED C++ / C# RAT] |

27.01.1401 A.P. — **PEGASUS** LIME HVNC [**LEAKED** C++ / C# **RAT**]. by - Apr 16, **2022**.

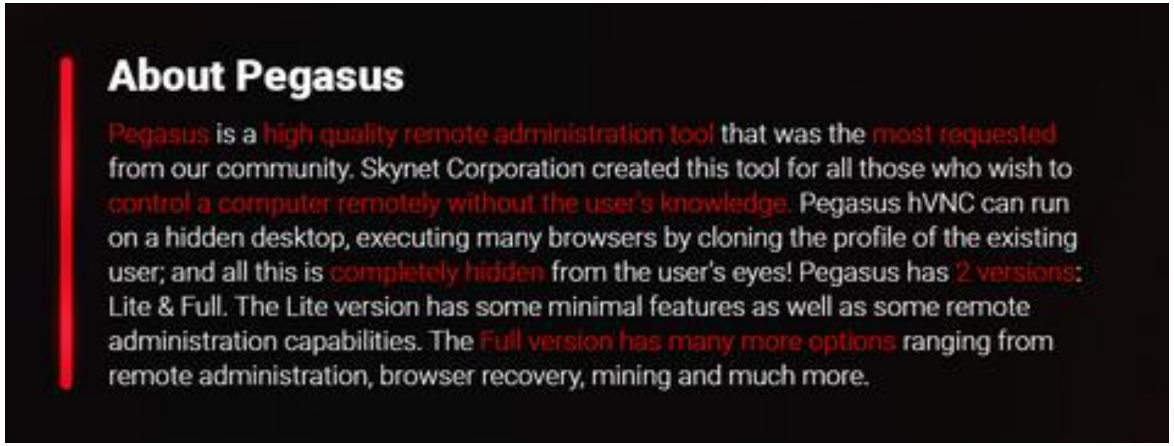


PEGASUS RAT FULL VERSION SOURCE!⚡ 1000$ RAT FULL SOURCE CODE LEAKED! ⚡2022⚡



SO THE SOURCE CODE OF THIS UHQ RAT NAMED PEGASUS WAS LEAKED!⚡ AND IT'S PROBABLY THE BEST RAT AVAILABE RIGHT NOW BECAUSE ITS A MIX OF ASYNCRAT, QUASAR RAT, AND DCRAT, VENOM RAT, ALL IN A SINGLE RAT, WITH EXTRA AND UNIQUE FEATURES!⚡TAKE A LOOK AT IT:

- Rootkit (Ring 3)
- Remote HVNC
- Remote Hidden RDPHrdp
- Hrdp Wallets Supported
- Remote Fun
- Remote Recovery
- Builder Features
- Remote System



About Pegasus

Pegasus is a high quality remote administration tool that was the most requested from our community. Skynet Corporation created this tool for all those who wish to control a computer remotely without the user's knowledge. Pegasus hVNC can run on a hidden desktop, executing many browsers by cloning the profile of the existing user; and all this is completely hidden from the user's eyes! Pegasus has 2 versions: Lite & Full. The Lite version has some minimal features as well as some remote administration capabilities. The Full version has many more options ranging from remote administration, browser recovery, mining and much more.

It is a cyber espionage tool. A tool that can take control of the device and exploit it according to the needs of the cybercriminal.

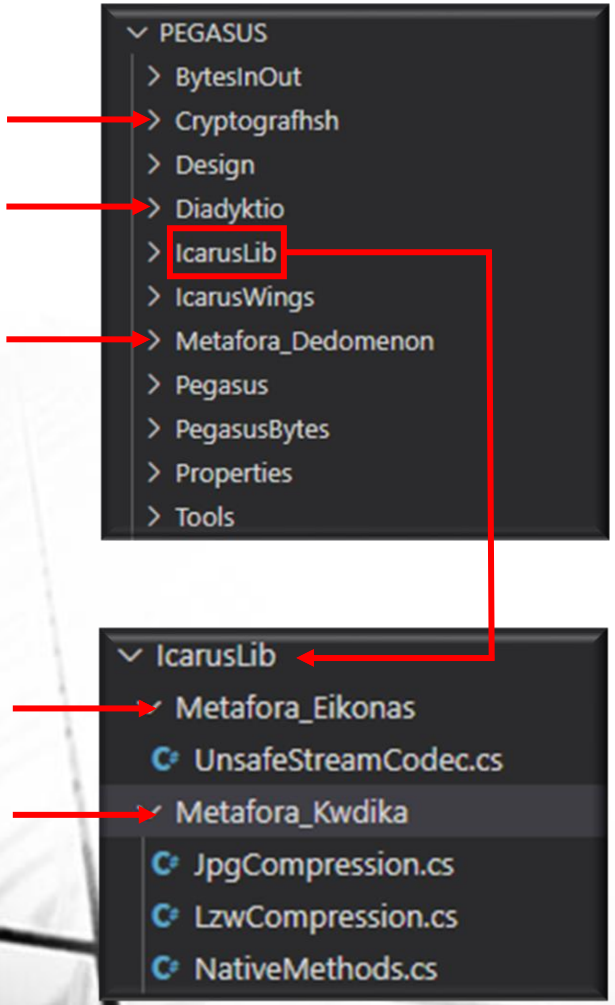
But going back to the real cyber espionage at the political, institutional or journalistic level, it is clear that the remote control tool options presented above does not make sense.

The leaked source

What about this information?

Analyzing the source code of this remote administration tool also brings surprises.

The PEGASUS folder contains subfolders with certain names.
For many it may not be visible, but some subfolders have interesting names.



```
PEGASUS
  > BytesInOut
  > Cryptografhsh
  > Design
  > Diadyktio
  > IcarusLib
  > IcarusWings
  > Metafora_Dedomenon
  > Pegasus
  > PegasusBytes
  > Properties
  > Tools
```

```
IcarusLib
  Metafora_Eikonas
    UnsafeStreamCodec.cs
  Metafora_Kwdika
    JpgCompression.cs
    LzwCompression.cs
    NativeMethods.cs
```

Cryptografhsh
(Κρυπτογράφηση)
=
Encryption

Diadyktio
(Διαδίκτυο)
=
Network

Metafora_Dedomenon
(Μεταφορά δεδομένων)
=
Data Transfer

What you see is Greek words written in Latin characters, a common case to Greeks for personal chatting, commercial and computer systems use, called Greeklish. From this we understand that one of the authors of the subsequent changes or even the author of the program may be of Greek origin. Not surprisingly, because Greece has many specialists in software development and cyber security.

Metafora_Eikonas
(Μεταφορά εικόνας)
=
Image Transfer

Metafora_kwdika
(Μεταφορά κώδικα)
=
Code Transfer

The leaked source

Maybe the next leak be the real
Pegasus Zero Click Spyware

According to the information presented, although it is a little disappointing that it is not the source code we wanted, we should still be glad that it is not.
In two days, the post on the Telegram has 6587 views, some of which may even be able to use the source code.

- We are used to the classic applications of cyber espionage.
- Antivirus applications are able to recognize hidden remote control activities.
- Through cybersecurity education, we are able to teach users how to recognize and avoid such attacks.

In the case of malware that is installed without the user intervening and through a simple SMS, the defense is more difficult.
So far only certain people have been targeted and all activity has been secret. What would we do with 50-100 cyber criminals who would have access to such technology?

Too bad we didn't find out the secrets of such malware, but it's better that the source code isn't public!

EDUCATION

... the best solution to start

"Privacy is the fountainhead of all other rights. Freedom of Speech doesn't have a lot of meaning if you can't have a quiet space. A space within yourself, within your mind, within the community of your friends, within your home, to decide what it is you actually want to say".

Edward Snowden

As an individual, you need and SHOULD safeguard your phone numbers, contact records, private conversation, medical records, financial records, etc. In the internet world, information is the real power, and those who have information have the power to rule.

EDUCATION

What you can do to protect

You MUST do what's right despite anyone else watching or not watching, caring or not caring!!!

You MUST have a plan to deal with unforeseen events!

As technology grows and becomes more complex and people integrate it more and more, cybercrime becomes a new way for criminals.

It is very difficult to prosecute cybercrime, because ....

Not everyone reports breaches.

Users/companies don't understand how much it can cost NOT to provide proper security.

EDUCATION

What you can do to protect

The best measure you can take is to keep updating our operating system, application or whatever updates the manufacturer offers!!!

On the other hand, an extreme measure would be to stop using applications and, most importantly, to NEVER browse social networks and emails through a browser. A phone's default browser is more vulnerable, so browsers like Google Chrome and Mozilla Firefox are better suited, because of constant security updates.
Even if it is not convenient, it will be safer, according to experts.

EDUCATION

How can we protect ourselves from this spyware?

Pegasus spyware is a big threat to individuals, as it can record data, spy the person’s private moments and sensitive personal data, without the knowledge and consent of the person who is being spied on.

Here are some useful tips that prevent spyware from getting into your device:

- Install a security application that checks and alerts if the device is insecure (rooted or jailbroken)
- Daily restart your device
- Disable iMessage
- Disabling Facetime
- Never click on links received via messages or e-mails
- Keep your mobile device up to date
- Install the latest security patches as soon as they are available
- Always use a VPN to hide your traffic (not a “free” one)

Alone, we are weak…

EDUCATION!!!

Together, we are strong!!!