CT2530: Lab # 5
Pegasus Spyware (PS) case study

Deadline
Please see the D2L dropbox.

Names of the students
Ryan Horwood

Introduction
This assignment aims to study the working of Pegasus spyware for academic purposes. Please look at the attached PDF downloaded from [1]. Students are strongly discouraged from building such a system, even for academic purposes. You can use the images from the report, but you need to cite them accordingly. Please write the answers in your own words. The total write-up (excluding the images and references) should be at least four pages. Please use this word file to write your answers, and don't change the spacing between the lines or the font.

Please note that, based on this lab, there will NOT be any questions final exam.

Questions
1) What are the benefits of Pegasus spyware (PS)?
   - Unlimited access to targets mobile devices: Get information about your target's relationships, whereabouts, calls, plans, and activities surreptitiously and remotely, whenever and wherever they are.
   - Intercept calls: Transparently monitor voice and VoIP calls in real-time
   - Bridge intelligence gaps: Gather new and different sorts of information to provide the most accurate and comprehensive intelligence, such as contacts, files, environmental wiretaps, passwords, etc.

- Handle encrypted content and devices: overcome any barrier posed by the complicated communications environment, including encryption, SSL, proprietary protocols, and others
- Application monitoring: Keep track of a variety of programs, such as Skype, WhatsApp, Viber, Facebook, and BlackBerry Messenger (BBM)
- Pinpoint targets: Use GPS to track targets and obtain precise positional data.
- Service provider independence: There is no requirement for collaboration with regional mobile network operators (MNOs).
- Discover virtual identities: Keep an eye on the smartphone always without bothering about frequently changing virtual identities or SIM cards.
- Avoid unnecessary risks: Remove the requirement for being physically close to the target or device at any stage.

2) Explain the high-level architecture of the PS.

The Pegasus system has levels to it. A complete cyber intelligence collecting, and analysis solution is formed by the combination of each layer, each of which has a specific role.

The following are the primary components and layers of the systems:

Installing new agents, upgrading old ones, and removing them are all responsibilities of the Installation layer.

Data collection is the layer in charge of gathering information from installed devices. Pegasus uses four kinds of data acquisition to provide comprehensive and complete intelligence:

Data extraction involves extracting all the device's data after agent installation, passive monitoring involves watching for new data to arrive, active collection involves using the

device's camera, microphone, GPS, and other features to gather information in real time, and event-based collection involves creating scenarios that automatically collect data.
Data Transmission: The Data Transmission layer oversees sending the gathered data in the fastest and safest manner possible back to the command-and-control servers.

Presentation & Analysis: This component's User Interface oversees giving operators and analysts access to the gathered data and transforming it into useful intelligence. The following modules are used to accomplish this:

- Real-Time Monitoring: Displays data gathered in real-time from one or more targets. When dealing with sensitive targets or during operational actions, where every piece of information that is received is essential for decision-making, this module is extremely significant.
- Offline Analysis: A sophisticated querying system that enables analysts to query and retrieve any gathered data. The sophisticated mechanism offers resources for uncovering connections and data that are buried.

- Geo-based Analysis: Displays the gathered information on a map and performs geo-based searches.
- Rules & Alerts: Create rules that send out notifications in response to certain data or events. Permissions, security, and health are all managed by the administration component, which is responsible for the overall management of the system.
- Permission: The system administrator can control the various system users thanks to the permissions mechanism. Give each person the appropriate level of access to only the data they are permitted to see. It enables the definition of groups in the

There are organizations that focus on just one or a few issues, and other organizations that tackle a variety of topics.

Security: The system security level is monitored by the security module, which also ensures that the acquired data is safely and securely placed into the system database for later inspection.

Health: The Pegasus solution's health component keeps track of each component's state to ensure that everything is operating as it should. It keeps track of how well the various components communicate, how well the system performs, how much storage is available, and informs users when something isn't working properly.

3) What is an agent? Explain how to install the agent on the device that is to be hacked.

The "Agent," a software-based component, is located on the end points of the targets being monitored, and its function is to gather the data for which it was configured. The most widely used mobile operating systems, including BlackBerry, Android, iOS (iPhone), and Symbian-based handsets, are all supported by the agent.

Each separate agent is set up to gather various pieces of data from the gadget and communicate it across predetermined channels within predetermined windows of time. The data is concealed, compressed, and encrypted before being transferred back to the Pegasus servers.

Once a dependable internet connection is established, the agent will communicate the data that is being continually collected from the device. When an agent is present, communications encryption, the usage of numerous programs, and other communications concealing techniques are no longer applicable.

REMOTE INSTALLATION:

Over-the-Air (OTA): The mobile device receives a push message secretly and remotely. The device downloads and installs the agent because of this message. No target participation or engagement is needed during the entire installation process (such as clicking a link or opening a message), and no warning shows on the device. The target cannot stop the installation because it is completely silent, invisible, and undetectable. Its NSO peculiarity notably sets the Pegasus solution apart from any other product on the market.

Enhanced Social Engineering Message (ESEM): The system operator might decide to send a conventional text message (SMS) or an email, enticing the target to read it, in situations where the OTA installation method is not applicable1. Installing a secret agent only requires one click, whether intentional or accidental. Although the target opened the link, they won't be aware that software is being installed on their device because the installation is completely covert. The likelihood that the target will click the link entirely depends on the reliability of the content. The Pegasus solution offers many possibilities for creating a customized and innocent message that will entice the target to open the mail.

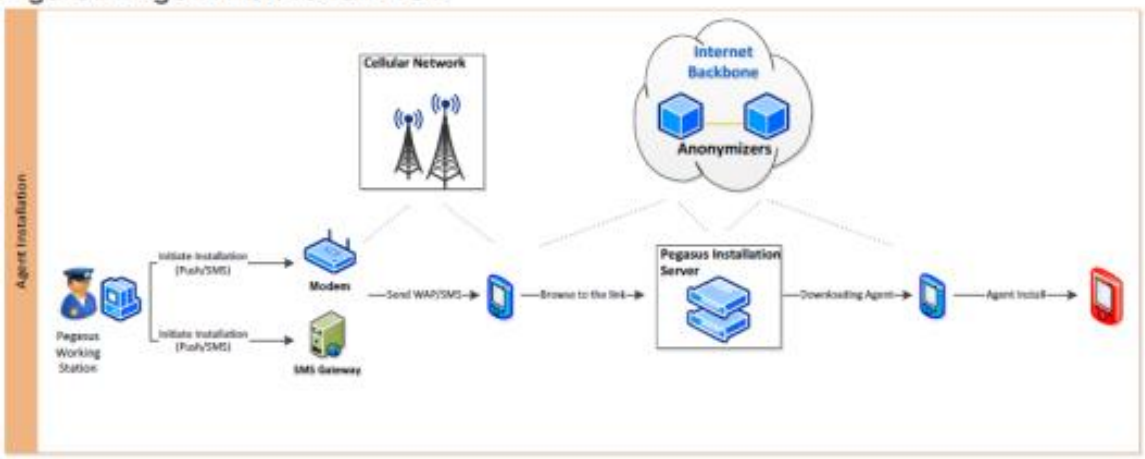
CLOSE TO THE TARGET:

Tactical Network Element: Once the number is acquired, the Pegasus agent can be silently injected via a tactical network device like a base transceiver station (BTS). The Pegasus approach makes use of these tactical tools' abilities to remotely inject and install the agent. Most of the time, assuming a position near the target is enough to complete the phone number acquisition. The installation is completed remotely as soon as the number becomes accessible.

Physical: The Pegasus agent can be manually injected and installed in less than five minutes when physical access to the device is an option. The same benefits as any other installation technique are provided after agent installation, including remote data extraction and future data monitoring.

4) Explain the agent installation flow in brief?

Figure 2: Agent Installation Flow



The Pegasus system operator merely needs to enter the destination phone number to start a fresh installation. The system takes care of the remainder automatically, usually culminating in the installation of an agent on the target device.

5) What kind of data could be collected once the device is infected with PS/ or when the device is ready to transmit the data to the PS server?

After the agent has been installed successfully, the device is monitored, and a variety of data is collected:

Information that is text-based includes text messages (SMS), emails, calendar entries, call logs, instant conversations, contacts lists, browsing histories, and more. Textual data is typically organised and compact, making it simpler to transfer and interpret.

Intercepted calls, outside noises (microphone recordings), and other audio recorded files are all examples of audio information.

Visual data consists of screen captures, photo retrieval, and camera snapshots.

Hundreds of items, including databases, documents, videos, and more, are present on every mobile device. Some of these files contain priceless intelligence.
 Location: Constantly tracking the device's location (Cell-ID and GPS).

Figure 4: Collected Data

References

[1] https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf