Interception Solutions

Introduction

The system is a leading cyber intelligence solution that enables government, law enforcement and intelligence agencies to remotely extract valuable intelligence from any IOT or mobile device.

This unique solution was developed to provide governments, law enforcement and intelligence agencies with tools to answer the new communications interception challenges in today's highly dynamic cyber battlefield.

The system gives the ability to collect all information from IOT and mobile devices, using new interception ways which enable a substantial technology gap to deliver the most accurate and complete intelligence for any security agencies.

The Interception Challenge

The rapidly growing and dynamic of the mobile communications market, bring new devices to the market, new operating systems and applications on a daily basis, which are being used by the targets who are aware of the interception technologies and systems being used by the governments and agencies.

To avoid the possibility of interception by the government or agencies, the targets change their devices and location on a daily basis, they close their phones during meetings and do not open any link which is sent to their phones.

These changes in the target's behavior and the communications landscape, requires a new thinking of the traditional intelligence interception tools, to be able to overcome on these challenges.

What are the Challenges

* Encryption: Use of encrypted devices and applications to convey messages.

* Abundance of communication applications: Sophisticated applications, most of which are IP-based and use proprietary protocols.

* Target outside interception: Targets' communications are often inaccessible (e.g., targets are roaming, face-to-face meetings, use of private networks)

* Use of various identities which are almost impossible to track and trace.

* Frequent replacement of SIM cards to avoid interception.

* Data extraction: The information is not sent over the network or shared with other parties and is only available on the end-user device.

* Complex and expensive implementation: As communications become increasingly complex, more network interfaces are needed. Setting up these interfaces

with service providers is a lengthy and expensive process and requires regulation and standardization.

What are today solutions

Until the above mentioned challenges are addressed and resolved, criminal and terrorist targets are likely "safe" from standard and legacy interception systems, meaning that valuable intelligence is being lost. The solutions being used today, as written below, deliver only partial intelligence, leaving the organizations with substantial intelligence gaps.

- Passive interception - Requires very deep and tight relationships with local service providers (cellular, Internet and PSTN providers). However, most contemporary communications is comprised of IP-based traffic, which is extremely difficult to monitor with passive interception due to its use of encryption and proprietary protocols.

- Tactical GSM interception solutions effectively monitor voice calls and text messages in GSM networks. When advanced cellular technologies are deployed (3G and LTE networks), these solutions become less efficient. In such cases, it is required to violently downgrade the target to a GSM-based network, which noticeably impacts the user experience and functionality.
- Malware presumably provides access to the target's mobile device. However, it is not completely transparent and requires the target's involvement to be installed on their devices. This type of engagement usually takes the form of multiple confirmations and approvals before the malware is functional. Most targets are unlikely to be fooled into cooperating with malware due to their high level of sensitivity for privacy in their communications. In addition, such malware is likely to be vulnerable to most commercially available anti-virus and anti-spyware software. As such, they leave traces and are easily detected on the device.
- Cyber intelligence, remotely and covertly intelligence from virtually any mobile device. This solution is able to penetrate popular smartphones operating systems by deploying invisible software on the target device. This agent then extracts and securely transmits the collected data for analysis. Installation is performed remotely (over-the-air), does not require any action from or engagement with the target, and leaves no traces whatsoever on the device.

Today systems – The problems

- Targets aware of the above technologies.
- Targets change their phones on a daily basis.
- Targets change their sim card on a daily basis.
- Targets off their phones during meetings.
- Targets change their location very often.
- Targets off their phones in their houses and offices.
- Targets do not open any link sent to their phones.
- Government/Agencies need to know the target phone number/IMEI/IMSI

Our System and its benefits

Our system offers law enforcement agencies and governments the ability to collect intel in many different ways and from many different devices at real time with a unique command and control backend that give the agencies many advanced cyber capabilities as they never had before.

All attacks within our system are done remotely by the agencies and do not require physical distance to target in order to conduct.

Some of our advanced features:

1. Many remote attack vectors: SMS, Email, WhatsApp, Telegram, Viber, or any other way that a link can be sent.

2. Supports many infection methods and many different devices such as: Mobile phones, Routers, Modems, DVR's, NVR's, Smart TV's, SIP phones, PBX and

many more IoT devices.

3. Both recon and attack mode gives the agencies both capabilities at real time, ability to collect full recon on targets internal network remotely ability to infect

any vulnerable device within that internal network.

4. Locate-Hear-See feature: state of the art capability to locate target while activating microphone at real time to hear the surrounding while system connects to

CCTV cameras around the location of the target to also see him in real time.

5. Intercept targets traffic remotely to collect data or manipulate network activities.

6. ONE command and control center for all devices and capabilities with correlation engine.

7. Bypass any encryption method used by targets such as: WhatsApp, telegram, signal, wicker and many more, even privately developed encryption applications.

Technology Highlights

In today's Cyber reality governments and law enforcement agencies use cyber capabilities and tools that are not fit or do not give the full the ever-growing evolution in technology.

As written above the targets are aware of the existing systems and use any tools available in the market to avoid detection

Our system gives a solution that does both recon and attack remotely.

Ability of interception the target without knowing his phone number/IMEI/IMS