11-28-2025

Cryptix Network | https://Cryptix-Network.org | info@cryptix-network.org

---

Surveillance and Zero-Day Exploits: How Governments and Advanced Attackers Bypass Encryption

Let’s talk about surveillance. It’s a sensitive topic and closely connected to hacking, so I’ll explain it in a simple and structured way.

1. Encryption protects data — but only during transmission

Many people believe that messaging providers secretly give governments backdoor access. In reality, strong end-to-end encryption (E2EE) protects messages while they are transmitted or stored on servers.

So how can governments, agencies, or hackers still read what someone writes?

They attack **before encryption happens**, by installing spyware or trojans on the device itself. Such tools can read the screen or capture keystrokes *before* the message is encrypted.
This means the attacker bypasses encryption entirely — these are highly advanced, targeted attacks.

---

2. Zero-Day Attacks

What is a Zero-Day?

A zero-day is an **unknown vulnerability** that developers have had “zero days” to fix. These vulnerabilities are extremely valuable, especially when they enable **zero-click attacks**, which do not require any user interaction.

There are two subtypes:

- **Zero-click attacks:** No tap, no link, no file opening required. The device is compromised automatically.

- **One-click attacks:** The attack triggers when a user taps a link, opens a file, or interacts with something once.

Zero-day exploits can be worth millions. iPhone exploits tend to be more expensive because iOS is closed source, making vulnerabilities harder to discover. Android is open source, so analysis is generally easier.

How an exploit chain works

A full compromise often involves several stages:

1. **Initial vulnerability** — for example, a buffer overflow
2. **Remote code execution** — the attacker runs their own code through that flaw
3. **Kernel-level privilege escalation** — gaining full control over the device

These chains can be zero-click or one-click, depending on the initial entry point.

---

3. How zero-days are discovered

Researchers and offensive security companies look for errors in software by stress-testing libraries and functions with huge amounts of input — for example, sending millions of malformed images or files to trigger crashes.
This can reveal vulnerabilities even without access to the source code.

Companies like NSO Group maintain large labs with hundreds of devices running automated tests to uncover memory corruption bugs and build exploit chains.

---

4. Pegasus and the NSO Group

NSO Group is widely known for **Pegasus**, a spyware tool that uses zero-click exploits to compromise phones — often without the user doing anything.
Pegasus is sold exclusively to **government agencies**, not to private individuals.

Its existence highlights the ethical problem: commercial profit from deeply invasive surveillance raises serious human rights concerns.

---

5. The Baseband — the smartphone's biggest weak point

One of the most vulnerable components in a smartphone is the **baseband processor**.

What is the baseband chip?

It is dedicated hardware responsible for:

- cellular communication (2G/3G/4G/5G)
- talking to the cell tower
- handling SMS and calls
- communicating with the SIM
- processing radio protocols

The baseband runs **independently** from Android or iOS and uses its **own firmware**.

Why is the baseband so dangerous?

- Attacks on it are often **zero-click by nature**
- Exploits can target huge numbers of devices simultaneously
- A baseband compromise can give very deep access to the phone
- Zero-days here can remain undetected for **months or even many years**
- Some exploits only work on specific devices, OS versions, or firmware builds, but baseband-level attacks cover a wider range

Security tip: Forcing the phone to use **4G or higher only** significantly increases safety, because older networks like 2G are far easier to exploit.

---

6. Summary

- Encryption protects data in transit, but **not** on a compromised device
- Zero-day exploits bypass user interaction and enable subtle, powerful attacks
- Spyware like Pegasus demonstrates how nations can target individuals despite secure apps
- The baseband processor is one of the most sensitive and least transparent parts of a smartphone
- Good digital hygiene and modern network settings can reduce risks