

THREAT RESEARCH: TARGETED ATTACKS ON ENTERPRISE MOBILE

INTRODUCTION

Recent high profile mobile threats and vulnerabilities like Operation Pawn Storm, xSSER mRAT, Masque Attack, WireLurker, Pangu, HeartBleed and more, are showing cyber thieves are making advancements toward mobile as an attack vector.

The line between consumer and enterprise mobile threats is blurry, but most IT Security executives recognize that they have mobile threats in their enterprise and this will be a growing concern for them as threats continue to evolve, putting enterprise data at risk.

For the enterprise, understanding the risk of these threats, while also enabling the visibility into them, is critical in order to protect against these vulnerabilities.

In an effort to better understand and quantify mobile threats in the Enterprise, Lacoon, in collaboration with Check Point, conducted a research study. The research was based on network communications in corporate Wi-Fi access points and also by measuring the most detrimental and meaningful threats for corporations.

This study focused on commercial mobile surveillance kits, also known as Mobile Remote Access Trojans (mRATs). mRATs top the list of mobile malware that customers are most concerned with from a risk and threat perspective.

These products are often marketed as child monitoring solutions, but we investigated an environment in which the legitimate uses of these products are very unlikely – the corporate environment.

When used maliciously, commercial mRATs can allow potential attackers to steal sensitive information from a device. they can take control of the different sensors to execute keylogging, steal messages, turn on video camera, and more. Attackers can target an enterprise and extract sensitive information from its employees' mobile devices.

EXECUTIVE SUMMARY

To determine whether or not mRAT threats are real for the enterprise, Lacoon used its analysis systems to supply Check Point with patterns and signatures that allowed Lacoon to see mobile devices communicating through corporate Wi-Fi access points with their command and control (CnC) server counterparts for more than 16 different mRATs of this type. Results follow.

KEY FACTS FROM THE REPORT

- Sampled more than 500k Android and 400K iOS devices
- Approximately 1,000 devices infected: 60% android, 40% iOS
- 0.12% of all the devices were infected with one of these mRATs
 - 0.21% for Large organizations in the US
- Corporate data at risk: emails, messages, keystrokes, calls, employee location
- Over 20 variants and 18 different mRAT families of products found
- Larger organizations are unevenly targeted by mRATs
- Over 100 countries were represented in this survey

METHODOLOGY

The Lacoon research team collected data from more than 500K Android and 400K iOS devices connected to corporate Wi-Fi through thousands of Check Point firewalls in over 100 different countries all over the world.

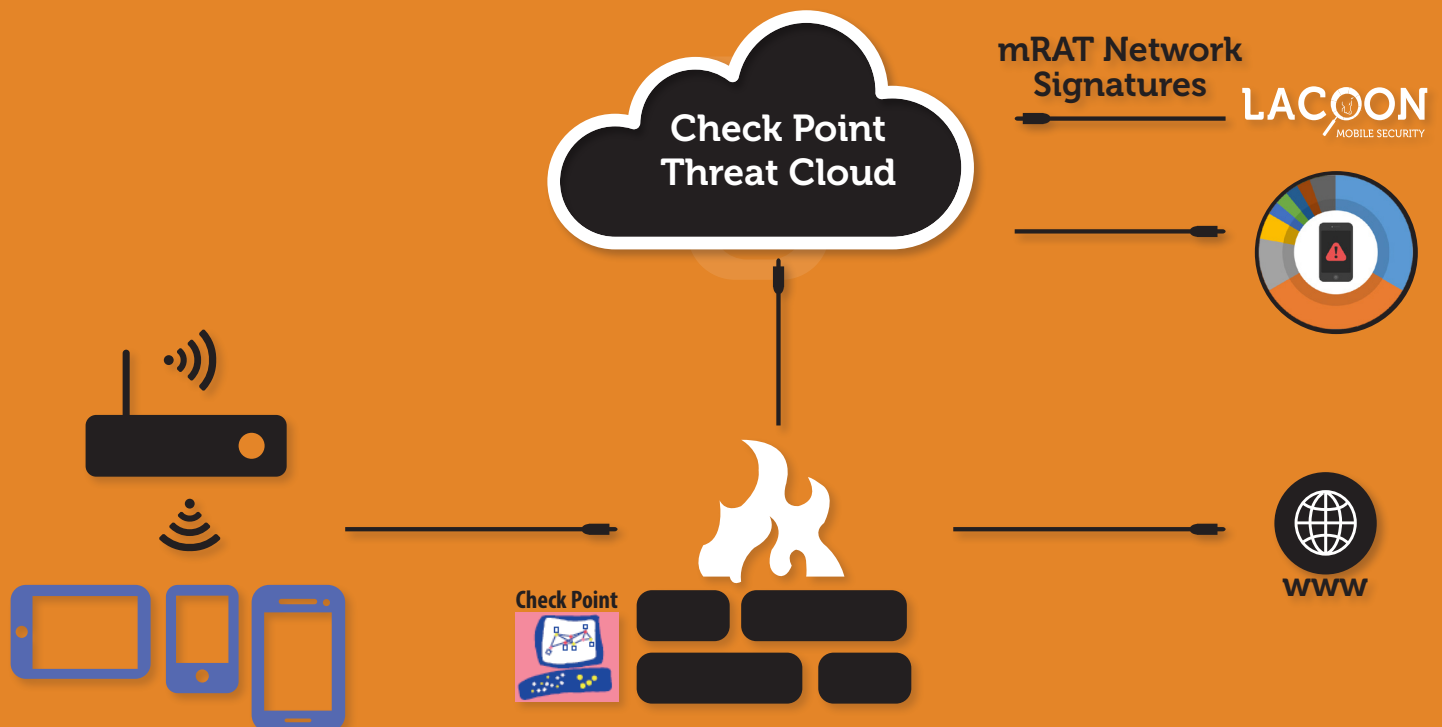
Starting in June 2014, and over a period of several months, Lacoon analyzed network connectors and looked for devices that connected through the corporate Wi-Fi and tried to communicate with an mRAT Command and Control (CnC) server. Devices that communicated with a CnC server were considered Infected.

Lacoon considered organizations with more than 2,000 devices as large enterprise-sized for its analysis.

Further Analysis Showed:

- Corporate employees have mRAT infections on their devices
- Enterprises are targeted by these products

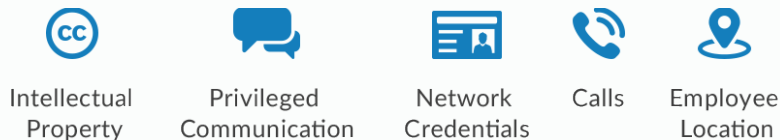
Methodology Workflow



ABOUT mRATs

Commercial mRATs are applications sold worldwide for the primary purposes of spying on people or monitoring children's safety. **mRAT** applications today are also used to steal commercial or enterprise data if installed on an employee's device without their knowledge. Because an **mRAT** enables administrative control, it is possible for an intruder to: track device location, use a key logger, activate device microphone, take screenshots, gain access to calendars, emails, 3rd party applications and more.










Corporate Data at Risk

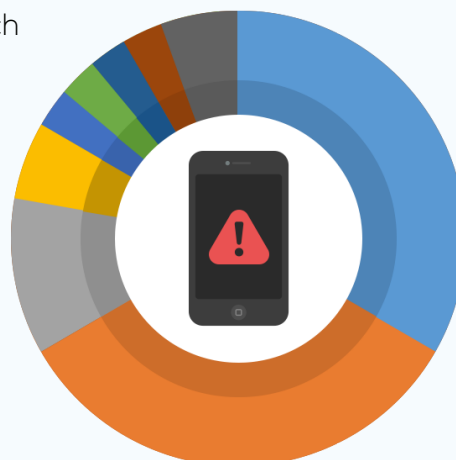


Commercial mRATs are usually installed on the device when the attacker is capable of gaining physical access to that device for a short period of time (such as a request to make a phone call or when the device is left on a table). **mRATs** can also be downloaded invisibly with a user-requested program, such as a game, or sent as a link through email or text.

Unlike most other malware, mRATs work on both Android and iOS. Also, they allow the attacker to take advantage of a very powerful set of capabilities on installed on a victim's device - unlike simple premium SMS, or the recent JPMC phishing attacks, which put only very small aspects of the owner's device at risk.

18 different mRAT families during this research

-  Mspy
-  Spy2Mobile
-  Bosspy
-  Mobile Spy
-  Shadow Copy
-  My Mobile Watchdog
-  MobiStealth
-  TalkLog
-  Others



RESULTS

Enterprises are targeted by mRATs

TWO TECHNIQUES WERE USED TO TEST THIS PROPOSITION:

- Infection rates across enterprises themselves
- The distribution of these infections

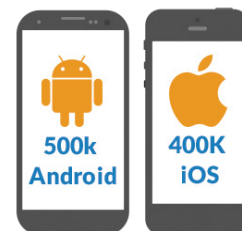
Are enterprises infected?

The data shows that employees of corporations are in fact targeted by mRATs. These infections have a high probability of malicious usage, as they are targeting corporate employees, not children. It was found that one out of every 1,000 devices was infected. Based on the dataset, if there are 2,000 devices or more in an organization, there is a 50% chance that there are infections within the enterprise network.

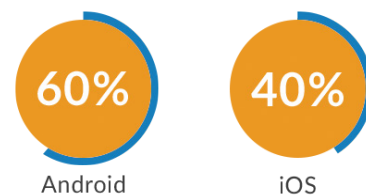
Are the infections distributed evenly?

The infections do not look uniformly distributed and are seen clustered in groups inside a partial group of the organizations reviewed and within countries.

SAMPLED MORE THAN



BREAKDOWN OF INFECTED DEVICES



The research shows fewer organizations are infected than expected, however those who are have significantly higher infection rates. In the US for example, there is double (0.31%) the rate of infected devices on gateways that show mRAT infections as opposed to the global infection rate of 0.15%

This points to the notion that not only are corporate employees being targeted, but certain organizations are themselves targets too, since the infections are clustered and focused in small parts of the overall group we examined.

The important message is that attackers choose certain organizations and attack multiple targets inside them, as opposed to just attacking corporate employees of random organizations and targeting them without relation to their organization.

Employees of targeted organizations have twice the chance of being infected by compared to employees of organizations which have not yet been targeted.

This is a meaningful problem for organizations. For companies with 2000 devices or more in the US, there is a 50% chance they will have 6 or more infected or targeted mobile devices in their network right now.

Top 10 Countries with mRAT Infections in Large Enterprises

