Madrid, August 2017

PandaLabs Records a 40% Increase in Attacked Devices this Quarter

- **The second quarter of the year has seen two of the largest cyberattacks in history: WannaCry and GoldenEye/Petya.**
- **We are currently witnessing the rise of advanced cybercriminal groups, the hacking of elections, the leaking of state-of-the-art espionage tools, and massive state-backed attacks that have brought us closer than ever to the brink of cyberwarfare.**
- **PandaLabs detected a 40% increase in devices targeted by unknown threats than in the previous quarter. El Salvador and Brazil are the two countries most likely to suffer an attack by new threats, with 10.85% and 10.04% respectively. At the opposite end is Sweden, with 0.42%.**

In their quarterly report, PandaLabs, the anti-malware laboratory at Panda Security, presents a rundown of the three most harrowing months in cybersecurity in recent years.

The Quarter in Numbers

This quarter has been defined by two major attacks: WannaCry and GoldenEye/Petya. The first infected over 230,000 computers in May and caused losses of between one and four billion dollars. The second, a sort of aftershock of the WannaCry earthquake, ended up affecting companies in more than 60 countries despite appearing to target primarily Ukraine.

The attack data analyzed by PandaLabs on all devices protected by one of Panda Security's solutions shows a 40% increase in attacks **from unknown threats** from the previous quarter. If we look at the type of client, home users and small businesses make up 3.81% of attacks, while in the case of medium and large companies the figure is 2.28%.

As for the **percentage of devices attacked in each country**, here are the ten most and ten least attacked:

Cybersecurity Trends

- **The most sought-after exploits are "zero-day" vulnerabilities,** which by definition are unknown and which allow attackers to compromise computers even if their software is updated.
- **Cyberwarfare:** WannaCry and Petya have shown us that government agencies won't hesitate to carry out large-scale cyberattacks, and that anyone on the internet could end up becoming a collateral victim of such attacks.
- **Ransomware** is still on the rise, and will continue to be as long as there are victims willing to pay.
- **Lost or stolen data** is a problem that is occuiring more and more frequently due to **human error or negligence**.
- **IoT y Smart Cities:** hyperconnected cities that are made up of networks of millions of devices will increase the overall reach of attacks, and the consequences will be more costly and more severe.

Traditional security solutions are not capable of dealing with attacks in which non-malicious tools and other advanced techniques are used. It is imperative to use security software appropriate to the level of threat that we are facing, such as Panda's own Adaptive Defense.

About Panda Security

Panda Security is the leading Spanish multinational in advanced cybersecurity solutions and in systems management and monitoring tools. Since its inception in 1990, it has consistently maintained a spirit of innovation and marked some of the most important advances in the world of cybersecurity.

Currently, the development of advanced cybersecurity strategies is the core of its business model. Panda Security has a presence in more than 80 countries and products translated into 23 languages, with over 30 million clients worldwide.