

# Panda Corporate Quarantine: Leveraging the community knowledge to reduce the Protection Gap.

October 2008.



**PANDA**  
SECURITY

*One step ahead.*

**Contents**

**EXECUTIVE SUMMARY .....3**

**THE REASON BEHIND THE CHANGE: THE NEW MALWARE LANDSCAPE .....3**

**COLLECTIVE INTELLIGENCE: A TOOL TO COMBAT THE NEW MALWARE DYNAMIC .....4**

**COLLECTION OF DATA FROM THE COMMUNITY .....5**

**AUTOMATIC PROCESSING OF DATA.....5**

*How does the Corporate Quarantine work?.....7*

**CONCLUSION .....8**

## Executive summary

As has been frequently pointed out by the security industry, the number of malware samples circulating today has increased alarmingly. So much so, that security companies have had to rethink the current protection model to adapt it and remain one step ahead of malware creators.

Panda Security detected this trend long ago, and in 2007 it had become a pioneer in the security sector with its Collective Intelligence, a new technology aimed at detecting ten times more malware with ten times less effort. This new approach improved our laboratories' processing of files and leverage of the community's knowledge thanks to a shift in mentality: the PC was no longer treated as an independent unit, isolated from the rest of computers in the world.

The basic benefits of the new Collective Intelligence approach are:

- Leverage of collective knowledge to proactively protect non-infected users.
- Automation of the malware protection cycle (sample collection, analysis, classification and remediation) to adapt to the new market dynamics. This technology improves detection of new unknown malware so that users are protected in real time from the moment a new sample is identified on a PC.

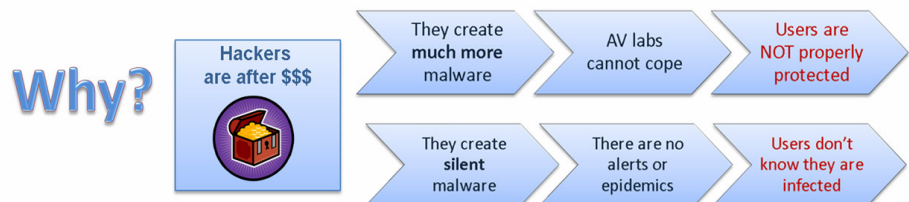
An important technology within Collective Intelligence is what we call Corporate Quarantine. This document aims at explaining how this technology works, and details the results obtained on our clients' computers since these new processes were implemented.

## The reason behind the change: the new malware landscape

It is a known fact that there are now more malware strains attacking computers than ever. This is mainly due to the appearance of an alternative market where malware creators can profit by creating and spreading malicious code. Now, it is not notoriety or fame that matters, but getting the malware to aid cyber-criminals in achieving their goals.



This new malware dynamic has led to the appearance of targeted attacks that remain hidden until they eventually manage to exploit unprotected users' weaknesses. Also, new techniques have appeared to improve and check the effectiveness of malware in remaining invisible to security products.



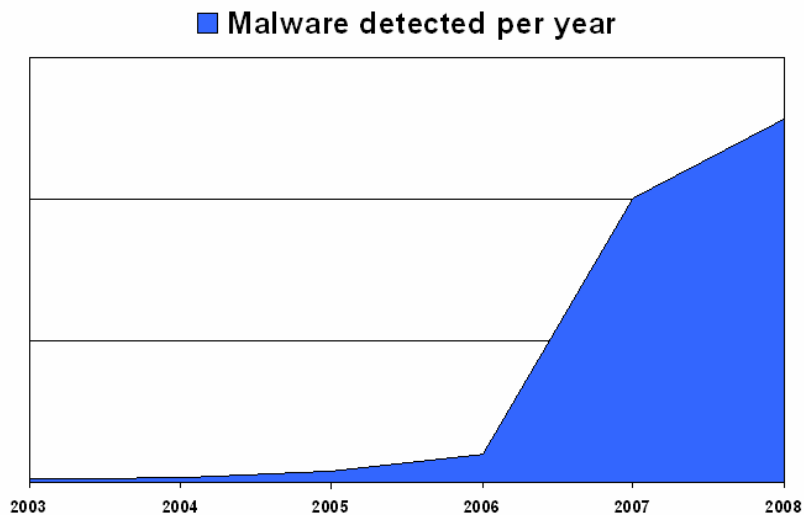


Figure 1: Unique malware samples detected from 2003 to 2008

### Collective Intelligence: a tool to combat the new malware dynamic

The whitepaper *“From Traditional Antivirus to Collective Intelligence”* published by Panda in August 2007 explained the model created by the company to combat the new global malware situation. This new model implied a shift in mentality regarding all current processes.

Why do we talk about a shift in mentality? Once it was clear malware laboratories couldn’t cope with the current volume of malware and it was impossible to protect users from zero-day attacks with traditional techniques, Panda started to change its internal structures to adapt all its solutions to the new landscape.

This resulted in Collective Intelligence, as represented in the diagram below:

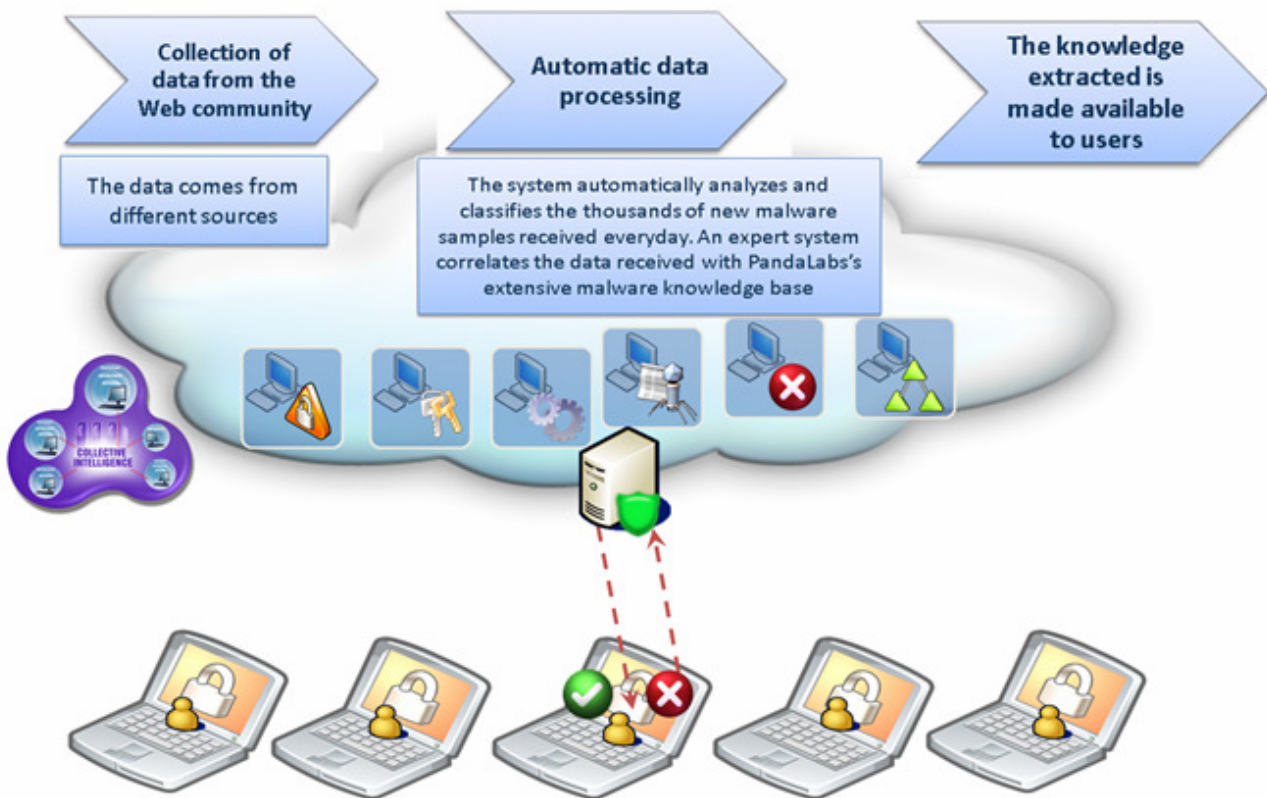


Figure 2: Graphic representation of Intelligence Collective

This new set of technologies comprises the following main characteristics:

**Collection of data from the community**

Until now, security solution architecture was based on the concept that users' PCs were independent entities, isolated from the rest of computers. Consequently, every malware strain detected on a computer would be considered apart from the rest. This approach prevented security companies from extending the knowledge about the evolution of each malware type as well as allowing other computers to benefit from proactive detection of specific samples.

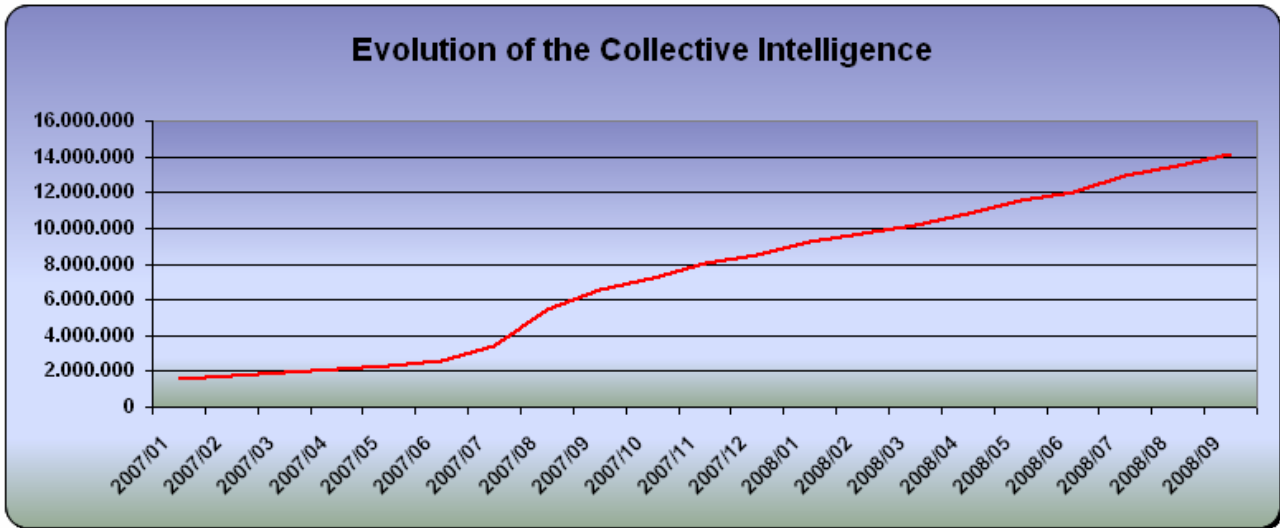
Thanks to Collective Intelligence, Panda has created a network of sensors and malware sources that extend our view of the current malware situation. This allows us to detect if a suspicious file is malware or not from the time it appears as well as spreading this knowledge across the user community in real time.

**Automatic processing of data**

Up to now, analyzing new malware samples presented several limitations. Firstly, samples had to be sent by clients to laboratories for analysis. Secondly, the analysis was subject to the availability of a lab technician that studied the sample and created a signature to distribute it to other clients. However, these tasks were not correlated, and so, when the number of malware samples started to grow disproportionately, malware laboratories became saturated and the time that passed between the appearance of a new malicious code and the reception of the corresponding signature by the clients started to increase.

We can resolve this thanks to the Collective Intelligence infrastructure. On the one hand we can collect, classify, and remedy malware automatically. On the other hand, this is an online process that takes place in a matter of seconds for the vast majority of samples. As a result, other users benefit from this knowledge in real time.

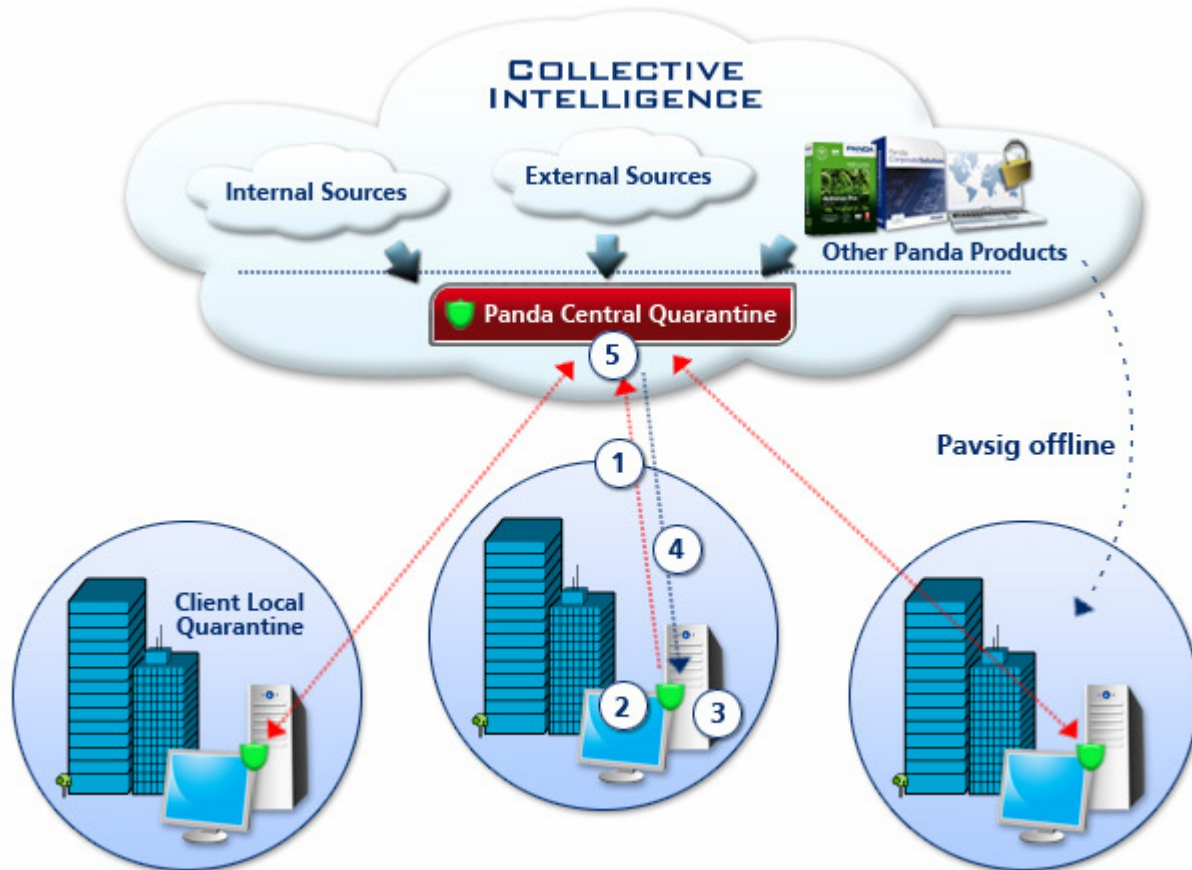
Since 2006, when the Collective Intelligence was firstly launched in experimental mode, Panda has been increasing its knowledge base year after year. From January 1, 2008, until now the number of known, stored files has increased by 63%, whereas in 2007 the number increased by 34.6% compared to the previous year.



One of the Panda technologies that has helped us most to adapt to the new malware landscape is what we call Corporate Quarantine. The purpose of this technology is to collect suspicious malware files from as many computers as possible in the most effective way so that we can process the myriad malicious samples detected on our clients' computers every day.

## How does the Corporate Quarantine work?

The diagram below shows the process taking place on a malware-infected computer.



### Step 1:

The Collective Intelligence agent on the client computer collects information about memory processes and objects and makes queries to the central CI servers, which check if the file is suspicious or not.

PandaLabs uses a network of over 4.000.000 of sensors to know which malware is currently in circulation and create the specific signatures to protect the user's PCs.

### Step 2:

If the file is found to be suspicious, the protection will mark it as such and send it to quarantine until a final verdict is passed on the file status.

### Step 3:

To optimize bandwidth consumption, the protection gets a 'fingerprint' of the suspicious file and sends it to the client's central console, which coordinates sending of samples to the CI servers, to find out if the file is a known suspicious file or not.

If a file cannot be identified, the CI servers notify the console, which sends the file together with information about it.

**Step 4:**

The file reaches the CI servers, where it is analyzed in-depth through a series of more sensitive technologies (sensitive heuristic analysis, signature analysis, emulation, sandboxing, virtualization, white lists, etc).

These servers apply proactive techniques which, not being limited by the resources of the users' PCs (CPU, memory limitations,...), can classify new malware samples automatically in a matter of minutes.

**Step 5:**

Once the file has been analyzed by our CI servers, two possible responses are returned, with different actions for each of them:

**5.1 The file is malware:** Information about the malware type is provided (worm, Trojan,...). Also, the protection treats the item according to the data received and the policies established by the administrator.

**5.2 The file is goodware:** The item is restored as it is known and it is not dangerous.

**Conclusion**

The last few years have witnessed a change in the way cyber-crooks think and act, exposing a series of flaws in the security industry.

Firstly, malware creators have found a way to profit from malware creation, which has brought about a change in their motivation. Now they launch targeted attacks that are far more effective than 'old' massive attacks that affected thousands of computers. This has saturated security laboratories, which cannot cope with the huge number of malware samples that they receive every day. Malware samples cannot be analyzed manually as in the past.

Finally, there is false sense of security, as massive attacks have been replaced with targeted attacks designed to go unperceived by the general public and anti-malware programs.

There are so many new malware samples in circulation that the time that passes between an attack on a user's computer and the analysis of the malicious code at the lab is used by hackers to infect other PCs without users knowing. In fact, our studies have shown that in 2007, 23% of users with an antivirus installed were infected with malware that their security solutions failed to detect. This data is part of the Infected or Not campaign launched by Panda to show this new malware trend ( [http://www.pandasecurity.com/infected\\_or\\_not/es/](http://www.pandasecurity.com/infected_or_not/es/) ). In March 2008 the percentage of infected PCs had dropped to 17%. Although this shows a certain reaction from the industry, there are still too many users with a false sense of security.

Thanks to the corporate quarantine, part of the new Collective Intelligence, Panda can reduce, to almost zero, the time during which users are left unprotected. Panda detects new malware from the moment it appears, transmitting the knowledge to all our clients in real time and protecting them against new threats.