

Ryan Sherstobitoff takes us into the AV lab at Panda Security USA

From Traditional Anti-Malware to Collective Intelligence

By Ryan Sherstobitoff

Recently there has been a lot of buzz concerning the latest reports on government entities being hacked, and in some cases their web sites are being defaced.¹ With the increase in sophistication and change in motivation of the attackers, I would not be surprised that some of these attacks were successful.

Web mafias and other foreign organized crime syndicates are of prime concern for businesses alike. With the advancement in malicious code and the increase in vulnerabilities discovered, targeted Trojans are being designed to penetrate defenses.

In fact, there is such a high volume of new and unique malware released on a daily basis by hackers and foreign organized crime groups that it creates a sustained denial of service against the resources at AV Labs. The result is more and more attacks that go unnoticed by the authorities until it is too late and confidential information of our nation's secrets have been stolen. This is mainly because specific malware (targeted or not) is not processed because of man-power issues relating to the DDoS attack on labs.

We call this the *Silent Epidemic* (which is referring to hidden attacks).

So how do we solve this problem? Partly by changing how security solutions are designed and deployed today. The traditional anti-malware model is simply not working: it is not providing effective protection against the 3000 + new threats received on a daily basis for several reasons:

1. Traditional signature-based solutions capture a small fraction of what is considered in "the wild." This is mainly because of architecture limitations – file size, bandwidth constraints, protection module design, etc.
2. The antivirus labs themselves do not have the manpower to process 100% of the samples received. Rather only a small percentage are included in the daily signature file.

3. Deploying protection upgrades in order to combat new malware strains is a difficult process in most part for large government and commercial agencies.

Data indicates that one out of five PCs will be infected with malicious code that their current security solution will not detect. Furthermore, a research study conducted here at the lab further confirms this with a 22% active infection rate out of a sample population of 1.4 million PCs. Thus, this leaves us with one pressing question: "Are we really protected?"

So where do we go from here?

1. Solutions must be developed to address the increase in malicious code
2. Protection should be designed to be easily upgraded
3. Automated methods and tools should be deployed within AV labs to analyze malware and reduce the manual burden

Security solutions developed to be hosted entirely on-line, which fit within the parameters of Web 2.0, would solve these problems by:

1. Reducing the manual effort required to process the thousands of samples received daily, thereby increasing the capacity and visibility that the lab has in terms of malware. The lab can see 10x more without the human effort involved to process each and every sample that comes in.
2. Allowing a much greater detection ratio through the development of web-based technologies that utilize signatures in "the cloud," rather than locally.

About the Author

Ryan Sherstobitoff is the Product Technology Officer at Panda Security USA (www.usa.pandasecurity.com). Ryan lectures across the USA on cybercrime trends as well as corporate risk assessments. He can be reached at ryans@pandasecurity.com.

¹ <http://www.securitypronews.com/insiderreports/insider/spn-49-20070924DHSBlast-sUnisysOverChineseHack.html>