White paper

AhnLab MDS :

Multidimensional Analysis of Malware
- The Answer to Advanced, Targeted Threats

AhnLab, Inc.

Table of Contents

Most cyber threats originate from outside networks and exploit known vulnerabilities. These attacks have been responded to via conventional security methods, such as with antivirus, firewall, and IPS solutions. However, more recent and sophisticated cyber-attacks have targeted organizations by injecting malware or files into web applications or email used by employees.

In 2012, Advanced Persistent Threat (APT) attack techniques evolved further to disguise executable files with common application icons, such as those representing a doc file. Users who believe that the file is safe then unwittingly launch a malicious executable by opening the file.

Other attacks involved customized malware that were distributed after first identifying a common operating system or application used by the employees at the target organization. In other cases, update servers for applications used by the targeted organizations were exploited for the distribution of malware or the malware was inserted into Windows help files (hlp). In others, malicious executables were included in compressed files, along with application installation files, hidden in plain sight.

One thing is common to all of these APT attack scenarios. Although the methods are diverse, all are triggered by malware. The attack initiates with the distribution of malware past conventional security solutions, which were unable to identify the unknown or variant codes. Because of this, many organizations remain vulnerable to APTs.

This paper introduces the differentiated malware detection provided by AhnLab Malware Defense System (MDS), which is capable of detecting unknown and variant codes accurately and efficiently. AhnLab MDS allows organizations to cope with advanced, targeted threats while protecting the essentials of business continuity.

Multidimensional Behavior Analysis

Malware analysis involves both static and dynamic techniques. Static techniques include analyzing external characteristics of a file, such as the PE header, or lines of code with professional tools like OllyDbg or IDA Pro. Dynamic techniques include analyzing sample files in a controlled environment, such as in a “sandbox” or virtual machine (VM) and monitoring changes in behavior.

Static analysis requires malware experts to spend a fair amount of time evaluating files. Dynamic analysis, on the other hand, requires very little time to uncover changes in the OS, such as network behavior, registry alteration, or file system alteration. False positives or false negatives can occur with dynamic analysis, but most APT response solutions employ it because it provides quick results. What’s more, dynamic analysis offers a means of identifying malicious characteristics of unknown or variant codes in a VM environment that is not available with signature-based solutions.

AhnLab MDS monitors known files, which account for more than 90% of the files flowing into the enterprise network, with the cloud-based AhnLab Smart Defense (ASD). The other 10% of unknown or variant files are assessed in a VM environment. As shown in Figure 1, to detect changes in the OS, the automatic API function hooking in the user mode and kernel mode of the VM are used at the same time as for notification routines that the system automatically calls when certain events occur.

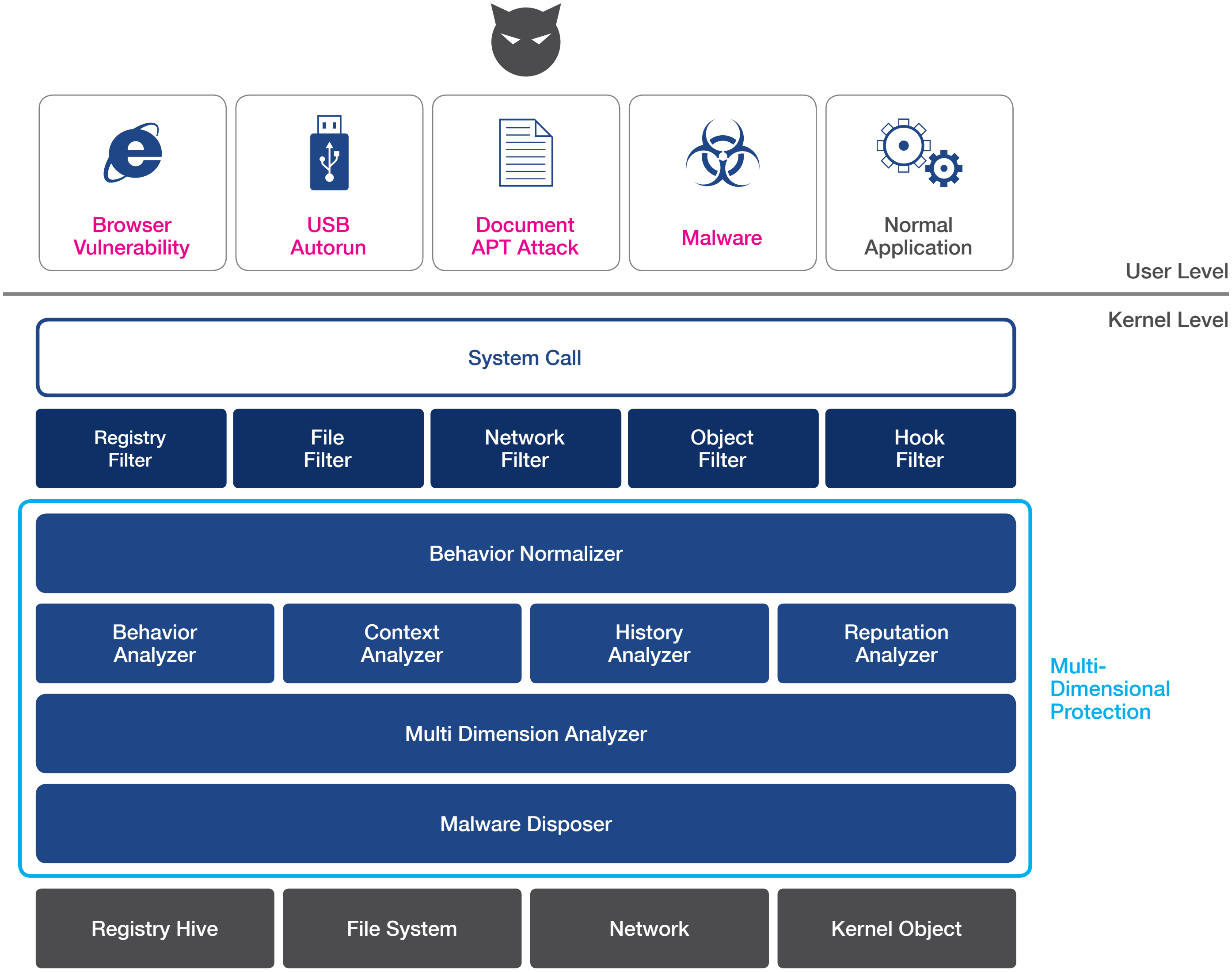


Figure 1: Architecture of AhnLab MDS' Behavior Analysis Engine

The most important benefit of AhnLab MDS is that most aspects related to file execution are considered when analyzing behavior. AhnLab MDS evaluates the results of the behavior analysis in combination with signature-based determination. Additional information about the associated files is reviewed. This includes malicious characteristics, the risk level of the URLs or IP addresses that the file connects to, reputation information, and comprehensive behavior patterns.

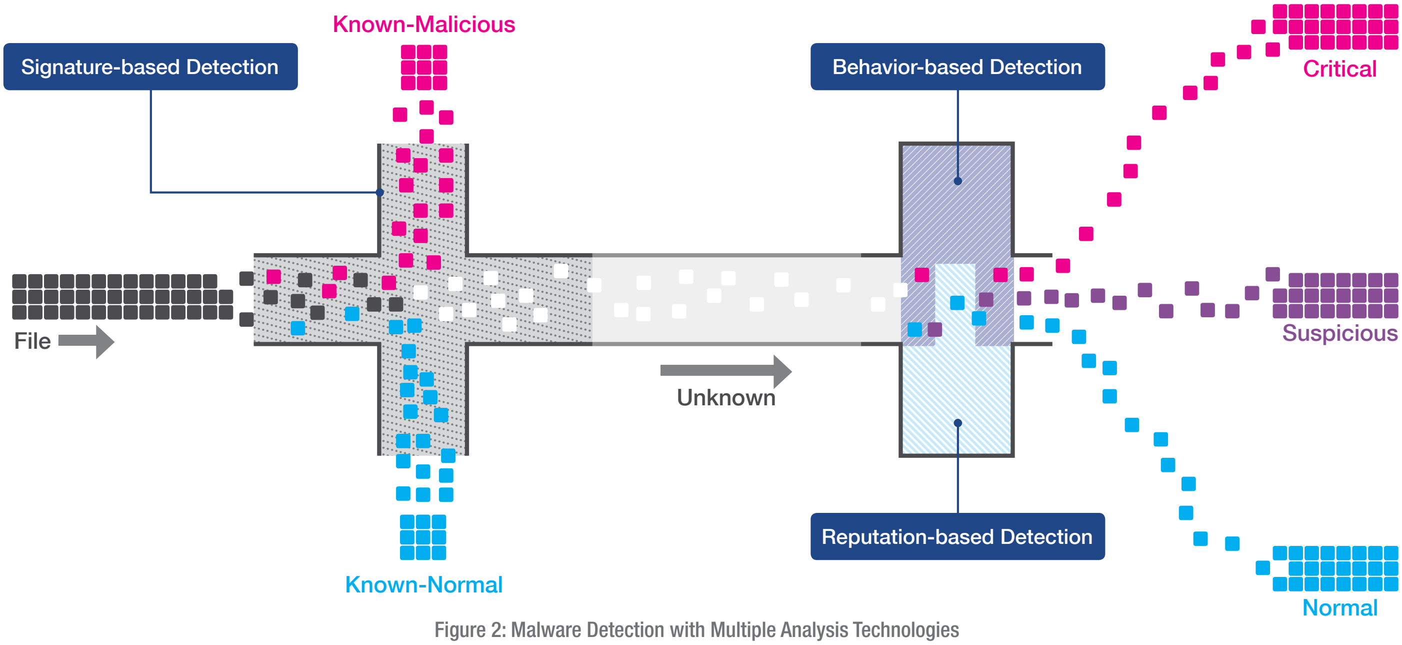


Figure 2: Malware Detection with Multiple Analysis Technologies

The reputation analysis method uses contextual information, such as source and collection time or the number of file users, to analyze both the sample file and associated files. This analysis technique has an important role in detecting targeted attacks that use unknown codes, because it allows for a more fundamental response.

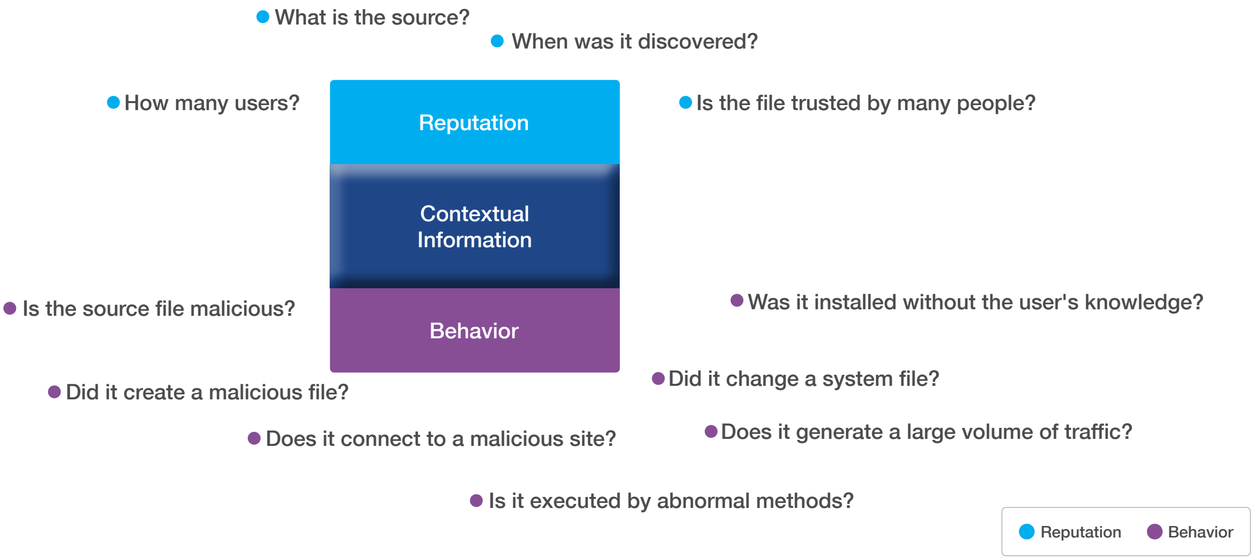

What is the source?
When was it discovered?
How many users?
Reputation
Is the file trusted by many people?
Contextual Information
Is the source file malicious?
Was it installed without the user's knowledge?
Behavior
Did it create a malicious file?
Did it change a system file?
Does it connect to a malicious site?
Does it generate a large volume of traffic?
Is it executed by abnormal methods?
Reputation
Behavior

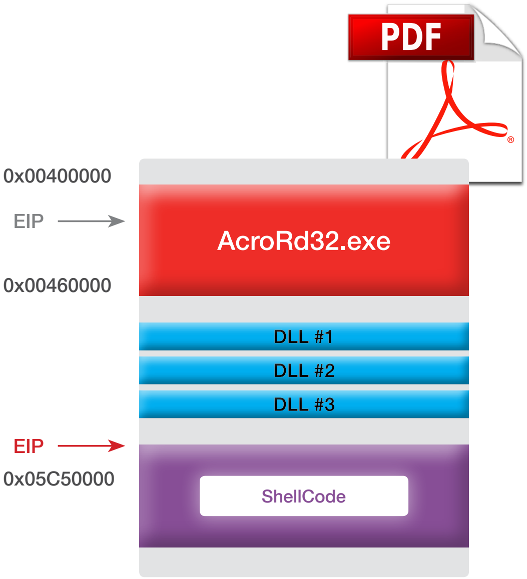
Figure 3: Behavior-based analysis and contextual information analysis based on reputation analysis

AhnLab MDS doesn't automatically flag malicious activity if suspicious behavior is found in the behavior analysis results. Instead, the differentiation feature minimizes false positive and negatives by considering the reputation analysis results (feedback from the AhnLab Smart Defense cloud feed).

Dynamic Intelligent Content Analysis (DICA)

The most salient feature of a targeted attack is that a web browser, web browser plug-in, or application like a text editor is used. Not so long ago, an attacker could damage a victim easily by attaching malware directly to an email or redirecting the victim to a malicious URL. However, this type of attack is no longer effective thanks to built-in security functions in web browsers or client email programs. As a result, attackers have focused their attention on non-executable files, such as documents. This is, because enticing a victim to open a pdf or doc (or one labeled as these) file that contains a shell code has a higher probability of success.

AhnLab MDS is equipped with Dynamic Intelligent Content Analysis (DICA) technology to detect an attack that uses non-executable files. DICA is AhnLab's patented application that performs both static and dynamic analysis of malware, which can directly verify malicious non-executable files in a VM environment.



Analysis Result	Malicious
Exploit Type	Exploit/PDF.AccessViolation-DE
File Name	C:\samples\sample1.pdf
Branch Module	C:\Program Files\Adobe\Reader 10.0\Reader\AcroRd32.exe
Branch Region	0x00400000 ~ 0x00460000
Shellcode Address	0x05C50000

Figure 4: Detecting a Shell Code with DICA

Figure 4 illustrates detection of a shell code inside a document file with DICA. Under normal circumstances, the extended instruction pointer (EIP) in the sample file should point from DLL #1 (0x7C930000) to DLL #3 (0x7C9CE000). However, the EIP in this file points instead to the area where the shell code is located (0x05C50000).

The information about the malicious file is also checked with behavior analysis to observe actions it carries out. With this multiple analysis technology, AhnLab MDS improves the reliability of its unknown file detection and diagnosis.

Cloud-based Analysis

Some APT response solutions emphasize signature-less analysis. This is based on the idea that APT attacks use unknown codes, which renders signature-based solutions useless. However, 90% of the files flowing into the enterprise network are either normal files or malicious files that use known codes. Furthermore, 25-50% of APTs utilize known malware, which means that signature-based malware detection technologies are useful for detecting a large volume of malicious activity, without needing to use more sophisticated analytical techniques.

AhnLab MDS detects threats efficiently by performing signature-based first, and then following up with other technologies, such as behavior-based analysis and dynamic content analysis, as shown in Figure 5. AhnLab MDS extracts the characteristics of a file to the “gray list” area, based on analysis information provided by AhnLab Smart Defense. Once these characteristics are extracted, additional static and dynamic analysis can be performed in the cloud, if necessary.

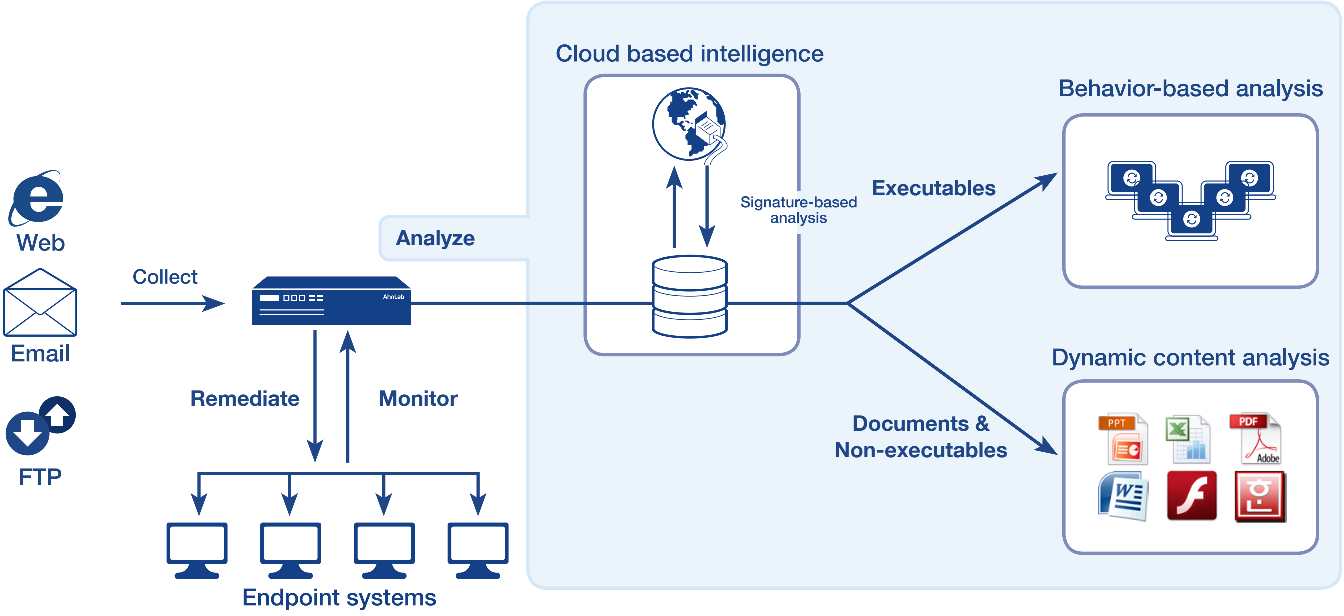


Figure 5: Malware Analysis with AhnLab MDS

Behavior-based analysis in the VM environment has some limitations. These include the CPU and memory load required to analyze a large number of files. AhnLab MDS identifies known malware with a blacklist and normal files with a whitelist, as shown in Figure 6. By utilizing the cloud-based ASD analysis information database, signature database, and real-time feedback, AhnLab MDS needs to use the VM environment only to detect unknown or variant malware. As a result, unnecessary analysis processes are minimized and AhnLab MDS performance is maximized.

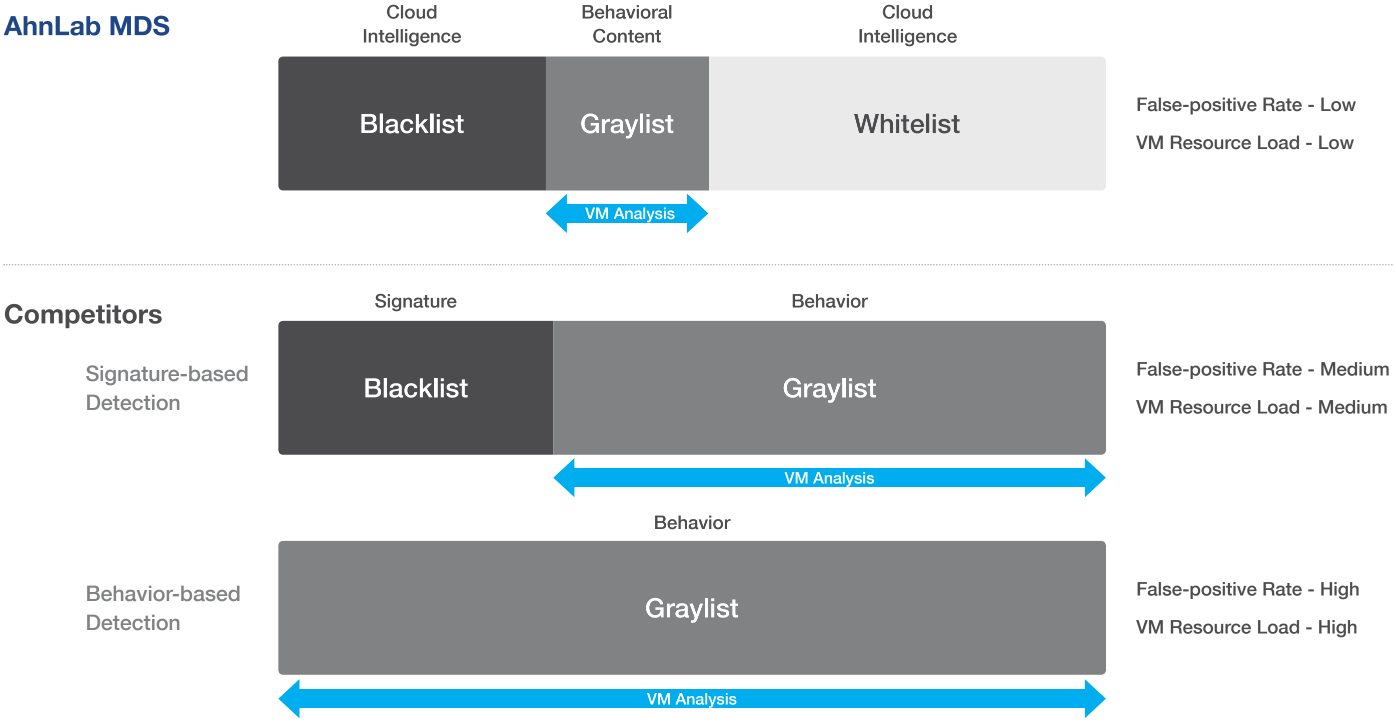


Figure 6: Comparison of False Positives and Analysis Performance

Conclusion

The frequency of APT attacks has been increasing sharply over the last few years. These techniques have evolved, and the targets have become wider in scope. Previously, APT attacks mainly aimed to steal confidential information. However, some of the more recent attacks have attempted to inflict serious damage on governmental agencies and critical infrastructures.

Despite these escalating threats, most organizations continue to respond with conventional security solutions, such as anti-virus solutions, intrusion detection/prevention systems, firewalls, Next Generation Firewalls, and web application firewalls. These organizations are limited by the time required perform multidimensional threat analysis, the inability of these devices to perform this analysis and the lack of an automated response to identified threats.

AhnLab MDS detects advanced malware from multiple angles with signature-based analysis, behavior based analysis, and dynamic content analysis. In addition, AhnLab MDS uses an automated threat response process that includes:

- Collection and analysis of data for all major internet protocols (HTTP, SMTP, and FTP)
- Two-way monitoring of traffic inflows and outflows on the network
- Monitoring and blocking harmful site access and Command & Control (C&C) communication
- Treating hosts that are suspected of infection (not just identifying them)
- Extracting suspicious files in the host

These capabilities are why AhnLab MDS is the best APT response solution to protect businesses including the enterprise from advanced, targeted threats. The business is protected, the employees are protected, and it frees up IT resources to focus on other business critical activities.

AhnLab, Inc.
2318-D Walsh Ave. Santa Clara, CA 95051 USA
Toll Free +1.800.511.AhnLab (1.800.511.2465)
+1.877.551.2690
Email info@ahnlab.com

AhnLab
Design Your Security