White paper

AhnLab Smart Defense:

The Solution to Complex Cyber Attacks

AhnLab, Inc.

Table of Contents

Introduction

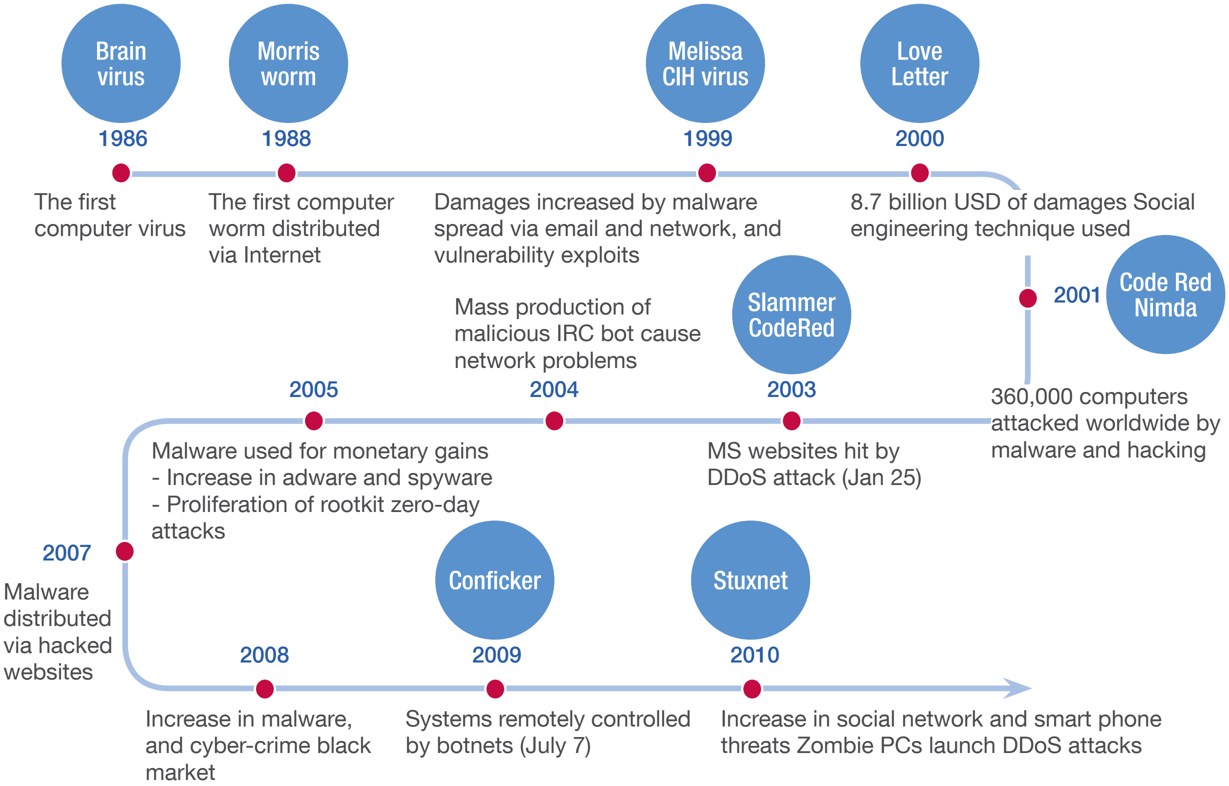
Since the first viruses and worms were distributed in the late 1980s, attackers and security companies have been going to new lengths to outdo one another. Attackers devise new types of attacks and security companies introduce new countermeasures to thwart them.

The problem with this cat-and-mouse game is that creating signatures to defeat malware in all its variations is a time-consuming and resource-intensive task. The cyber-security industry needs a more responsive, more proactive approach to cope with ever-increasing threats to commercial and personal data.

In this white paper, AhnLab introduces a new solution, based on cloud computing technology, automated threat analysis, and DNA maps of malware characteristics identified from a database of almost 500 million code samples. The AhnLab Smart Defense (ASD) system delivers fast, proactive detection and prevention of threats, while simultaneously reducing the time and resources required for updates.

Security Threats on the Rise

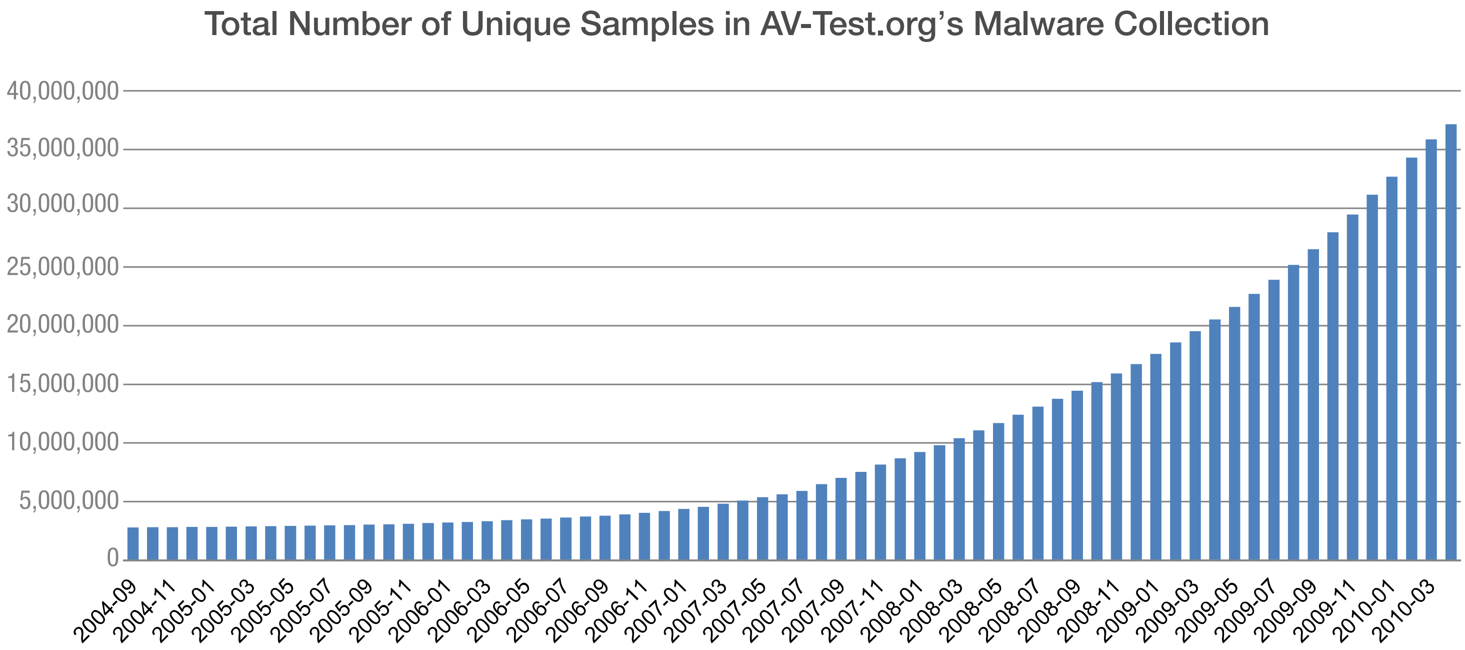
Traditionally, hackers wrote malicious scripts to satisfy their curiosities and demonstrate their coding skills. More recently, these motives have shifted, as attacking and remotely controlling systems have become a widespread and profitable criminal endeavor.


Brain virus
1986
The first computer virus
Morris worm
1988
The first computer worm distributed via Internet
Melissa CIH virus
1999
Damages increased by malware spread via email and network, and vulnerability exploits
Love Letter
2000
8.7 billion USD of damages Social engineering technique used
2001
Code Red Nimda
360,000 computers attacked worldwide by malware and hacking
Slammer CodeRed
2003
MS websites hit by DDoS attack (Jan 25)
Mass production of malicious IRC bot cause network problems
2004
2005
Malware used for monetary gains
- Increase in adware and spyware
- Proliferation of rootkit zero-day attacks
2007
Malware distributed via hacked websites
2008
Increase in malware, and cyber-crime black market
Conficker
2009
Systems remotely controlled by botnets (July 7)
Stuxnet
2010
Increase in social network and smart phone threats Zombie PCs launch DDoS attacks

Evolutionary History of Malware

From 2005, waves of new cyber attacks have given rise to a black market where personal identities, bank account numbers, and credit data are bought and sold like legitimate commodities. As the profitability of these crimes increases, so does the number of malware produced. Furthermore, the cyber-crime black market now includes easy-to-use malware authoring tools that reduce the skill level and experience needed to produce malware variants.

According to data published by AV-TEST Institute, a worldwide provider of security testing and consulting services, the number of unique malware in their collection has risen dramatically in recent years, from around 3 million in 2004 to nearly 37 million in 2010. AhnLab's Security Emergency Response Center (ASEC) reported more than 170 million malware distributed worldwide in 2011 alone.

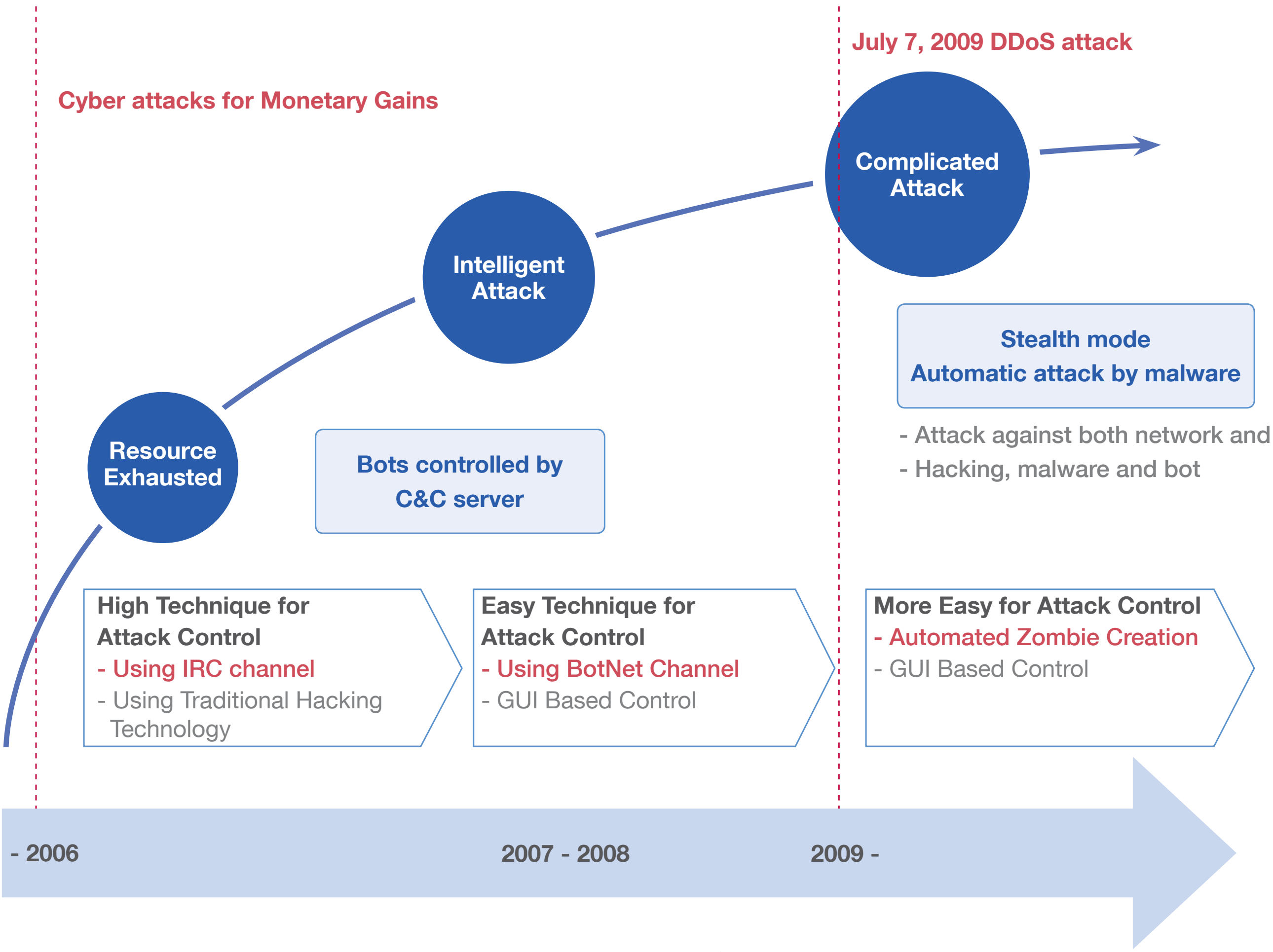


Upward Trend of Malware Production
(Source: AV-Test.org)

A New Breed of Attacks

As the profitability of cyber crimes has increased, distributed denial-of-service (DDoS) attacks have undergone significant changes. Early DDoS attacks aimed to exhaust system resources, usually through TCP SYN flooding or UDP/ICMP flooding to create 1-3 GBps of traffic. Beginning in 2007, DDoS attacks were carried out by botnets controlled by a Command and Control (C&C) server. At this point, GUI-based malware authoring tools became available on the cyber-crime black market, which allowed a greater number of hackers to easily create malware and launch cyber attacks with them.

On July 7, 2009, a massive DDoS attack hit websites of the South Korean and US governments. The pattern of this attack was novel, in that zombie PCs were used to launch attacks on the targeted websites at pre-designated times. This more sophisticated approach allowed the perpetrators of the attack to conceal themselves more effectively behind the botnets.


July 7, 2009 DDoS attack
Cyber attacks for Monetary Gains
Complicated Attack
Intelligent Attack
Resource Exhausted
Stealth mode
Automatic attack by malware
- Attack against both network and PC
- Hacking, malware and bot
Bots controlled by C&C server
High Technique for Attack Control
- Using IRC channel
- Using Traditional Hacking Technology
Easy Technique for Attack Control
- Using BotNet Channel
- GUI Based Control
More Easy for Attack Control
- Automated Zombie Creation
- GUI Based Control
- 2006
2007 - 2008
2009 -

Evolution of DDoS Attacks

Current Security Solutions Fall Short

The explosive increase of malware has resulted in new problems for makers of anti-malware products. Since the cyber attack on July 7, the industry has seen a rise in compound attacks that compromise both endpoints and networks. Security companies have largely been indecisive about how to combat these comprehensive threats with one-dimensional security solutions.

According to the data published by AV-TEST, security companies are being quickly outpaced by the introduction of new malware. While the number of new malware increased over an average of 150 times in 2010 compared to that of 2005, the number of signatures/program updates only increased by 5 times.

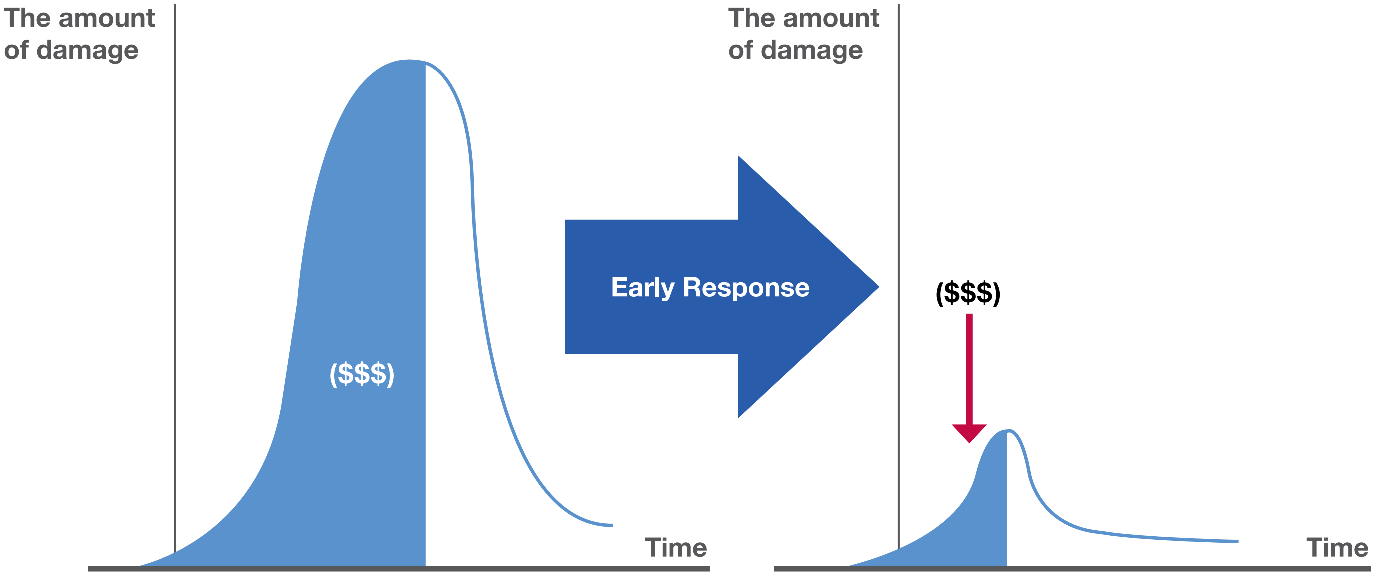
Year	2005	2010
Signature/Program Updates		
per Day	110	574
per Month	Over 3,400	Over 17,000
per Year	Over 40,000	Over 200,000
New Malware		
per Day	360	Over 50,000
per Month	Over 10,000	Over 1,500,000
per Year	Nearly 130,000	Nearly 20,000,000

Increase in Malware vs. New Signatures (Source: AV-Test.org)

Confronted with growing limitations in their existing anti-malware technologies, major security companies have added techniques such as heuristic detection, proactive prevention, and sandboxes, to their traditional signature-based detection approaches. Unfortunately, these methods do not cover all types of security issues, due to the diversity of computing environments, the difficulty of managing frequent update releases, and the risk of false-positive results.

Slow Responses Cost More

With the number of malware increasing rapidly, timely updates take on increased importance. Anti-malware companies continually attempt to shorten update cycles, but it takes time to collect malware samples, analyze them, develop new signatures, and distribute updates. During this turnaround period, systems are vulnerable to zero-day attacks and the amount of damages incurred can escalate rapidly before a countermeasure is released. As seen in the below figure, illustrates, an early response would significantly reduce the cost of damages caused by most malware.



Early Responses Reduce Damages

More Resources Needed

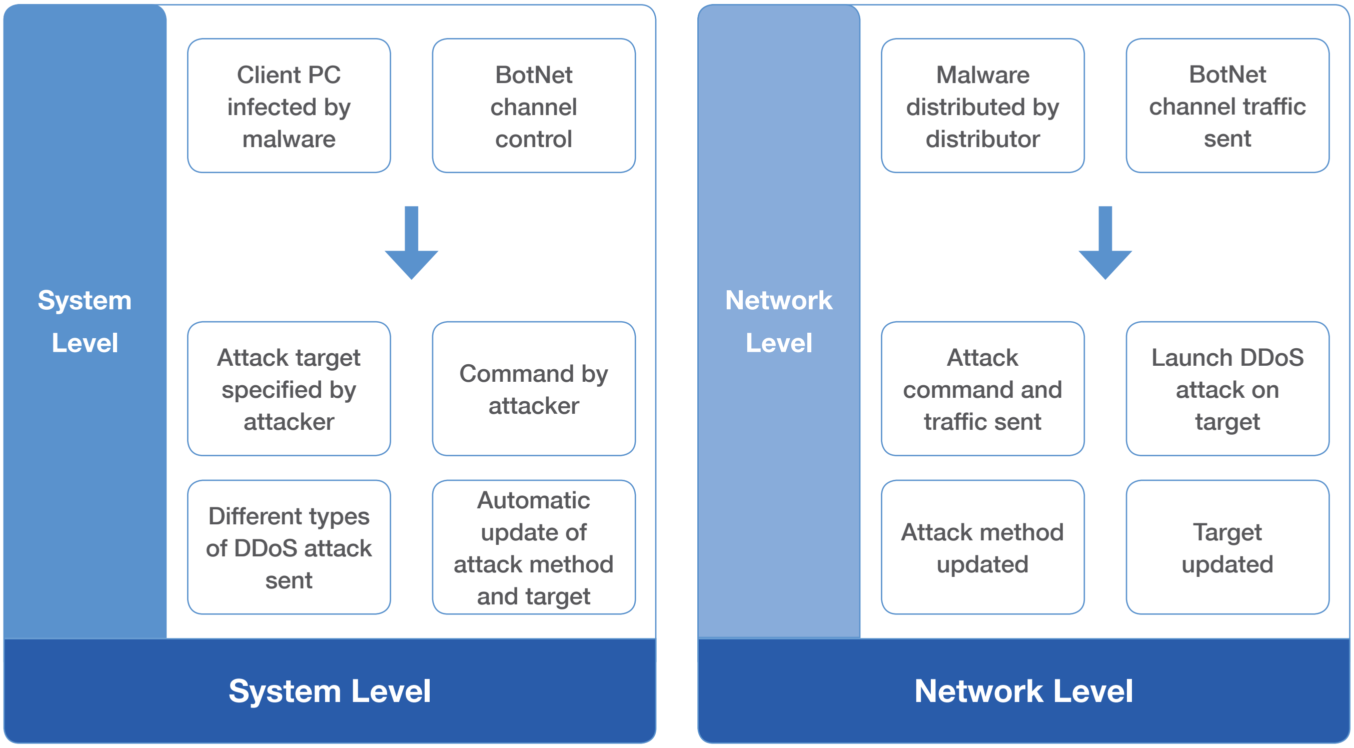
Another limitation with current solutions is the amount of resources needed for updates—adding more signatures to cope with new malware results in increased engine sizes for anti-malware programs. AV-TEST reported that resources required by most anti-malware programs increased by 15 times on average from 2005 to 2010. At these rates of growth, it is obvious that the amount of available hardware resources becomes a significant factor in keeping computers updated

Year	2005	2010
Size of the Updates		
per Day	1.2 GB	17 GB
per Month	Over 30 GB	Over 500 GB
per Year	Over 400 GB	Over 6,120 GB

Growing Update Sizes (Source: AV-Test.org)

Incomplete Network Security Solutions

Network security products maintain the integrity of the network and service availability by blocking unauthorized access and malicious inbound traffic. However, they are incapable of quarantining infected computers located on the network to prevent them from spreading malware. Recent DDoS attacks have taken advantage of vulnerabilities at both system and network levels. Without the ability to respond to attacks that originate at the system level, network security products cannot prevent repeated attacks.

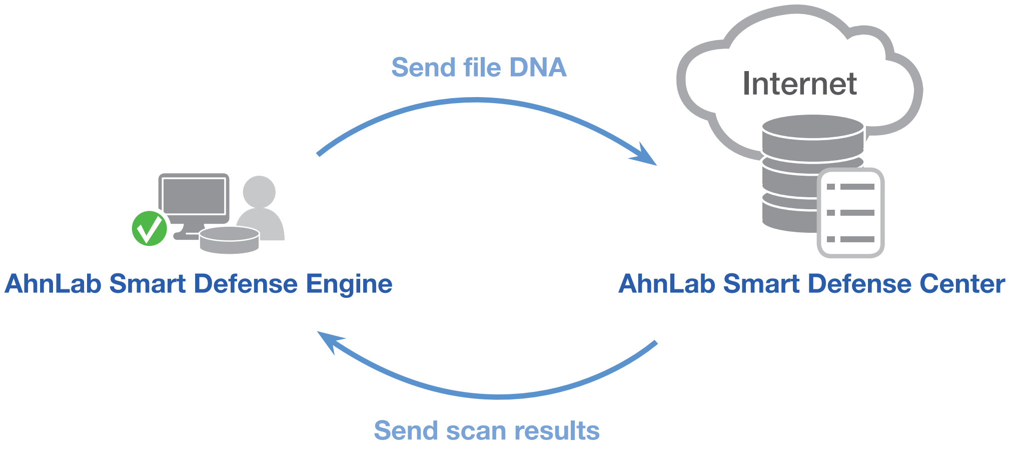

System Level
Client PC infected by malware
BotNet channel control
Attack target specified by attacker
Command by attacker
Different types of DDoS attack sent
Automatic update of attack method and target
System Level
Network Level
Malware distributed by distributor
BotNet channel traffic sent
Attack command and traffic sent
Launch DDoS attack on target
Attack method updated
Target updated
Network Level

Characteristics of DDoS Attacks (System vs. Network Level)

AhnLab Smart Defense (ASD)

AhnLab's Smart Defense System provides a legitimate solution to the problems with today's current security environment. This cloud-based system drastically improves response time, reduces the need for system resources, and closes the gap in network security to protect against DDoS attacks.

Released in 2009, ASD is AhnLab's first cloud-based security solution. It consists of an ASD engine installed on local computers and the ASD Center located on AhnLab's servers. Its server-side databases are hardware and platform-independent to provide consistent, widespread protection from security threats and reduce the need for physical storage on local computers.



ASD Components

Customized, Automated Responses

ASD provides advanced protection by scanning files on local computers and communicating with the ASD Center via the internet. It then delivers customized protection for local machines and automated threat analysis to reduce the need for local resources and accelerate response times:

1. After completing the first scan, a customized signature database that corresponds with local files is stored as a cache on the local computer. Subsequent scans will only check new or modified files against this personalized signature and skip unchanged files to increase scanning speed.

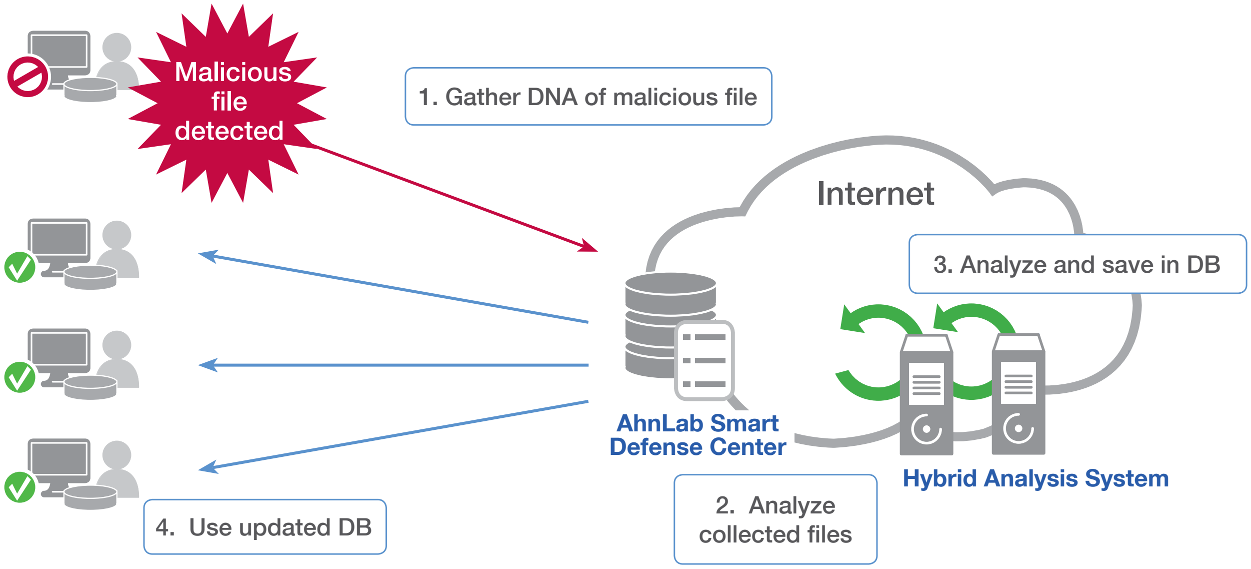
2. If an unknown file is found, the file's DNA information (a digital fingerprint of the file's characteristics) is transmitted to the ASD Center for analysis.

3. The ASD Center checks the file's DNA against the current database. If it finds a match, the ASD Center updates the customized signature database on the local computer to inform the ASD engine whether the file is malicious or legitimate.

4. If no match for the file's DNA is found on the database, the information is transmitted to the automatic analysis system. Transmitted information contains executable information only and does not include any personal information.

5. The automatic analysis system determines whether the file is legitimate or malicious through a variety of techniques, including analysis of the basic file information and the program's digital signature, reputation-based analysis, behavior-based analysis, and correlation analysis.

6. Analysis results are transmitted to the ASD Center and the database is updated. This new update is immediately available to all ASD users.


Malicious file detected
1. Gather DNA of malicious file
Internet
3. Analyze and save in DB
AhnLab Smart Defense Center
Hybrid Analysis System
2. Analyze collected files
4. Use updated DB

ASD Workflow

Agile and Effective

Unlike other security solutions, the ASD system allows for real-time responses to unknown malware. Hundreds of thousands of code samples are reported daily to ASD from several million users and the analysis results of those samples are reflected in the database almost immediately. ASD's Hybrid Analysis System (HAS), with its automatic file analysis, makes it possible to analyze and distribute new signatures in a fraction of the time required by human virus analysts.

With its server-side database, ASD can quickly identify and respond to emerging threats, without having to rely on traditional, time-consuming update cycles. And, ASD's ability to create personalized signature databases on local machines means scans for new malware waste no time scanning known, legitimate files.

When ASD detects sudden increases in network traffic or the use of large amounts of network resources over a short period of time, it monitors the file for malicious activity and makes it possible to take appropriate steps to limit damages. Assuming that a DDoS attack is likely to follow, ASD tracks the malware distribution path and relays the botnet's IP information to other security devices and firewalls, so that DDoS attacks can be blocked effectively.

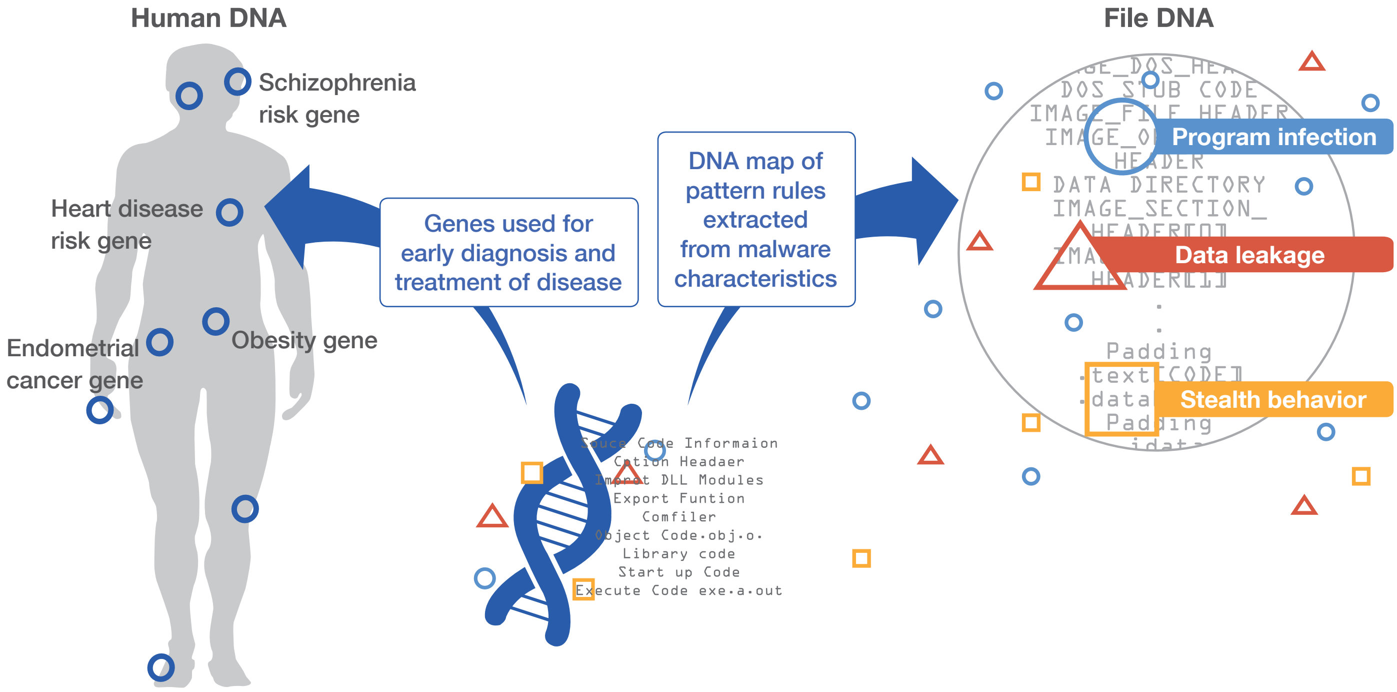
Date	Filename	Size	ASD Detection	Score	ASDP	Count
2010-08-20 10:17:27	maychi.exe	96,256	Backdoor/Win32.Bredolab	100	100	1
2010-08-20 10:14:57	1620040ee1fc903af62debd...	187,904	Trojan/Win32.Hiloti	100	100	
2010-08-20 10:14:55	nabi[1].exe	141,824	Downloader/Win32.Forbid	100	100	8
2010-08-20 10:14:30	zaimpactstrength.exe	766,464	Trojan/Win32.Sadenav	100	100	
2010-08-20 10:13:27	cqldrllkl.exe	768,000	Trojan/Win32.Sadenav	100	100	
2010-08-20 10:11:43	exe.exe	85,504	Trojan/Win32.FakeAV	100	100	
2010-08-20 10:11:40	ddf437b511ec25d4a5e5c56...	98,304	Trojan/Win32.FakeAV	100	100	
2010-08-20 10:11:06	d23dcd17811ea7eae84fc4b...	94,720	Backdoor/Win32.Bredolab	100	100	
2010-08-20 10:10:10	63f74d72e676435b6b22b91...	61,440	Trojan/Win32.FakeAV	100	100	
2010-08-20 10:08:01	CDROM.SYS	84,800	Trojan/Win32.Patched	100	100	1
2010-08-20 10:06:29	sample.exe	35,840	Trojan/Win32.CSon	100	100	
2010-08-20 10:06:04	apr.exe	3,858,432	Dropper/Win32.AdrenaPatched	100	100	3
2010-08-20 10:06:04	kgh.dll	48,012	Trojan/Win32.FraudPack	100	100	
2010-08-20 10:05:38	kgh.dll	48,012	Trojan/Win32.FraudPack	100	100	
2010-08-20 10:05:06	A057RE18.dll	643,584	Trojan/Win32.Overtls	100	100	1
2010-08-20 10:02:10	C_WINDOWS_apsesf.dllx	77,312	Trojan/Win32.Hiloti	100	100	
2010-08-20 10:01:47	C_WINDOWS_system32_a...	20,480	Trojan/Win32.Bredavi	100	100	
2010-08-20 09:59:30	qney.exe	194,048	Trojan/Win32.OnlineGameHack	100	100	1
2010-08-20 09:59:29	14a38041e080a3cf22b6c4c...	96,768	Backdoor/Win32.Bredolab	100	100	
2010-08-20 09:58:01	C_WINDOWS_help.dllx	94,208	Backdoor/Win32.Cindyc	100	100	

Sample of Malware Identified by ASD

ASD Uncovers the DNA of Malware

AhnLab analyzed the inherent similarities between types of malware and their variants and found that all malware has its own digital fingerprint that distinguishes itself from legitimate software. Just as flesh-and-blood criminals can disguise their external appearances but cannot change their DNA, malicious codes contain identifiable characteristics that cannot be altered. The ASD solution incorporates DNA Scan technology to interpret these characteristics and identify malware, regardless of how they are disguised.

The DNA Scan is based on 20,000 DNA rules and 800 million samples stored in the ASD database. Based on extracted characteristics, AhnLab derived a DNA map to recognize pattern rules of legitimate and malicious codes. This approach overcomes the limitations of signature-based detection methods and provides a highly effective, proactive solution for blocking malware that minimizes false positives with almost no additional hardware resources required. The DNA Scan is implemented on both the server and client machines, so that DNA rules can be applied even when a network connection is unavailable.



The DNA of Malware

Fast, Accurate Identification

In a conventional one-to-one response method, 6 million signatures are required to block 6 million malware. The DNA Scan method, on the other hand, can block the same number of malware with as few as 1,000 signatures by applying pattern rules to identify common malware characteristics. Even when the DNA scan is applied alone, without updated signatures, it is capable of detecting more than 90% of ARP spoofing tools. It is also capable of blocking codes created by the same author by reflecting characteristics such as coding style or frequently-used functions in the pattern rules.

The DNA Scan technology marks a significant improvement over other detection methods by reducing the risk of false positive identifications. Pattern rules are distributed only after comparison and verification against more than 300 million legitimate and trustworthy files that are updated daily in the ASD database, to ensure the validity of detection results. By incorporating the DNA Scan rules into the its antivirus software, AhnLab was awarded the VB 100% Award, for zero false positive results, from the international testing and certification institution Virus Bulletin. The detection rate was also improved, as a result of ASD's server-based approach combined with the DNA Scan's proactive response capability.

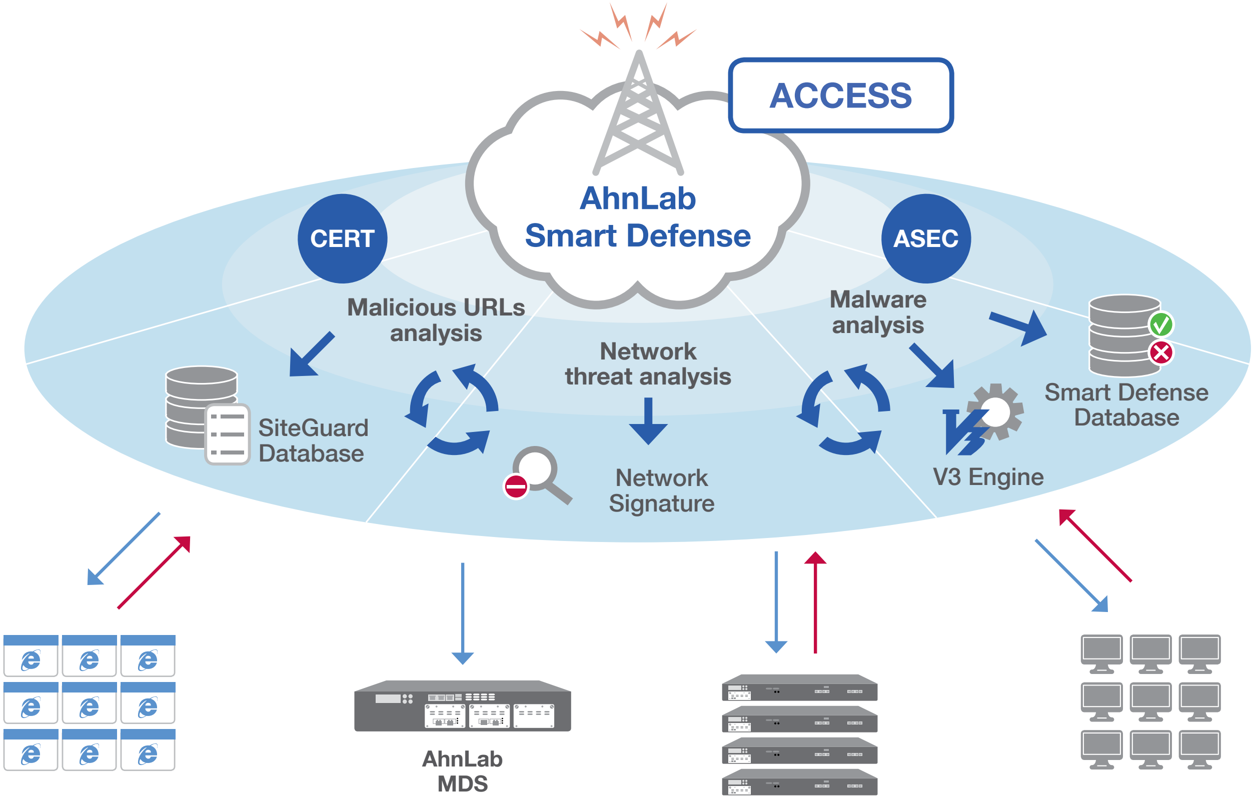
Synergistic Collaboration

ASD and the DNA Scan complement each other perfectly. ASD collects and analyzes an enormous number malicious and legitimate software samples, the DNA Scan decodes characteristics and establishes pattern rules from information transmitted to the ASD Center, and all of this data is housed conveniently in the ASD Center. This synergistic approach provides a fast, effective, and accurate response to emerging malware and overcomes the limitations of the traditional update cycle for signatures.

In user environments where the network connection is intermittent or unstable, or even when the user cannot access the Internet, or is working where file transmission is prohibited with a strict security policy, the DNA engine can still scan and identify malware locally on the computer.

This redundancy in the ASD system ensures that users are provided the best possible protection, without sacrificing resources, and in spite of changes in the connectivity environment.

ASD is at the core of the AhnLab Cloud Computing E-Security Service (ACCESS). This integrated threat management platform that combines cloud-based antivirus protection with expert human resources, such as the malware collection and analysis capability of the AhnLab Security Emergency Response Center (ASEC) and the threat monitoring and response service of the Computer Emergency Response Team (CERT).



AhnLab Cloud Computing E-Security Service (ACCESS)

Conclusion

With the introduction of tools that make it easier to create malware and the increased profitability of cyber crimes, cyber attacks will continue to pose an enormous economic and social threat. For example, some industry analysts estimate that the damages caused by the DDoS attack in 2009 surpassed 50 million USD, while an earlier attack, in January of 2003, was estimated to have caused damages in excess of 155 million USD. Faced with explosive growth in the number of new malware, it is no longer feasible to create, test, and distribute the volume of signatures necessary to address these security threats. Furthermore, these cyber attacks are taking on new levels of complexity that make single-point security solutions ineffective.

The AhnLab Smart Defense System (ASD) provides a proactive, multi-dimensional solution to today's advanced security threats. Hosted in the cloud, ASD reduces the demand for system resources on client computers and increases scanning efficiency through customized signature databases for local machines. On the server side, ASD implements the Hybrid Analysis System (HAS) to quickly identify malware and develop signatures in a fraction of the time required by human virus analysts. The rapid response of ASD increases the likelihood of preventing attacks and limiting damages.

ASD takes security to a new level by incorporating DNA Scan technology. Based on characteristics extracted from more than 300 million samples in the ASD database, the DNA Scan uses pattern rules to block millions of malware with a small set of signatures. The DNA Scan provides a redundant layer of security and rounds out a synergistic approach that keeps pace with elevating threats, while improving detection rates and minimizing false positive results.

AhnLab has integrated ASD into the core of the AhnLab Cloud Computing E-Security Service (ACCESS), an integrated threat management platform that combines cloud computing with the expert human resources of the AhnLab Security Emergency Response Center (ASEC) and the Computer Emergency Response Team (CERT). This strategy is designed meet today's dynamic security requirement, ensure business continuity for our clients, and contribute to a safer computing environment for all.

About AhnLab

AhnLab creates agile, integrated internet security solutions for corporate organizations. Founded in 1995, AhnLab, a global leader in security, delivers comprehensive protection for networks, transactions, and essential services. AhnLab delivers best-of-breed threat prevention that scales easily for high-speed networks, by combining cloud analysis with endpoint and server resources. AhnLab's multidimensional approach combines with exceptional service to create truly global protection against attacks that evade traditional security defenses. That's why more than 25,000 organizations rely on AhnLab's award-winning products and services to make the internet safe and reliable for their business operations.

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-400, Korea
www.ahnlab.com / global.info@ahnlab.com / Tel: +82-31-722-8900

AhnLab
Design Your Security