Security Trend

2016 REVIEWS &
2017 PREDICTIONS

AhnLab

CONTENTS

2016 Threat Reviews

- The Top 5 Security Threats that Engulfed 2016

2017 Threat Predictions

- Top 5 Security Threats that Will Sweep Over 2017
- Advices to Combat Security Threats in 2017

Security Trend

2016 REVIEWS &
2017 PREDICTIONS

AhnLab

2016 Threat Reviews

The Top 5 Security Threats that Engulfed 2016

AhnLab

The Top 5 Security Threats that Engulfed 2016

Ransomware, the Threat That Locked Up the Whole World

The different types of ransomware increased abruptly in 2016, causing enormous damage worldwide. According to ASEC (AhnLab's Security Emergency-response Center), ransomware-related security breaches reported only 15% of the total cases at the beginning of the year, but became 60% of the total by the end of 2016.

Ransomware threat evolved through continuous changes and spontaneous or deliberate extinctions. TeslaCrypt announced they were shutting down their activities in 2016, and CryptXXX has been quiet since July 2016. On the other hand, Locky and CERBER have been constantly upgraded. New types of ransomware that encrypts MBRs (Master Boot Records) to interfere with the use of the PC itself, have also appeared.

The so-called Ransomware-as-a-Service (RaaS), ransomware services that generate and disseminate ransomware for profit, have started to pick up steam and accelerate the spread of ransomware in 2016. In addition, dissemination and infection methods are being diversified constantly. Attaching files to spam, drive-by downloads, malvertising, Remote Desktop Protocol (RDP), and combining social engineering techniques are becoming more advanced.

The Top 5 Security Threats that Engulfed 2016

Targeted Attacks, Cost-efficient with No Boundaries

Targeted attacks have increased significantly over the past few years due to their cost-efficiency. These attacks generally directs at national agencies and companies with political or financial purposes.

The security incident of the US Department of Homeland Security's personnel information in February 2016, is widely suspected to have been the work of Russia. The security breach on the NSA by the Shadow Brokers organization August 2016 is also linked with international espionage.

Targeted attacks directed at individuals usually have political purposes: Targeted attacks were mostly directed at politicians or social activists who oppose the ruling parties in countries such as Hong Kong, Myanmar, Syria, the UAE, and Kazakhstan.

The traditional cyberattacks on companies involves stealing customers' personal information. In 2016, two large-scale personal information attacks were carried out on Yahoo and Dropbox. Also, the business email scam, a conventional e-mail falsification, caused tremendous damage to companies in North America and Europe, and is still ongoing. According to FBI reports, there were around 7,000 cases of email falsification in the US, resulting in losses of $7,400,000 in 2016.

The Top 5 Security Threats that Engulfed 2016

The Preemptive Attack of IoT Malware

As Internet of Things (IoT) technologies advance, so do IoT-related threats. IoT devices use embedded Linux systems, which are lightweight in terms of usability and feature low power consumption. The reality is that Operation Systems used by user terminals are not easy to manage, and security is often overlooked, particularly by small manufacturers. Attackers have not missed this point.

In September 2016, record-breaking DDoS attacks were carried out against security blog Krebs on Security and the hosting company OVH. A US Internet hosting service provider, Dyn, was also the target of DDoS attacks. This attacks took advantage of connection problems on websites such as Twitter, The New York Times, Airbnb, PayPal, Netflix, SoundCloud, and others. It was confirmed that both attacks utilized the IoT malware, Mirai. Various IoT devices were exploited in this attack and more than 10,000 IoT malware were discovered alone in 2016 after the source codes of some malware was released to the public.

Recently, IoT device manufacturers have started to pay close attentions to security. However, it is not easy to constantly monitor IoT devices once purchased and installed. Assuming they will be used for 5 years after installation, attacks using IoT devices can occur any time during the operation period.

The Top 5 Security Threats that Engulfed 2016

Survival of the Fittest: Fierce Attacks via Exploit Kits

The Exploit Kit (EK) is a tool that distributes large quantities of malware that target vulnerabilities. The Exploit Kit is becoming more and more active as the ransomware black market grows. There has also been fierce competition between Exploit Kit developers.

Angler EK and Nuclear EK, which were the most distributed ransomware programs in the first half of last year, suddenly disappeared, and the activity of Neutrino EK, which inherited the position of Angler EK, also decreased in the second half of the year. On the other hand, Sundown EK and Magnitude are still constantly active.

The Exploit Kit's multilevel redirection technique is mainly used to distribute different kinds of malware (including ransomware) in malvertising attacks. The distribution of both downloaders with different script formats and Exploit Kit-based ransomware is constantly distributed. People have even discovered malware that uses Windows Powershell.

Also, as the use of the Exploit Kits increases, distinct vulnerability attacks have grown stronger, including those that exploit the vulnerabilities of Internet Explorer, Flash, and Java. Particularly, there has been an increase in the distribution of malware that exploits the vulnerabilities of Encapsulated PostScript (EPS), which is related to document files, and Open Type Font. It was also discovered that AtomBombing, a code injection technique that exploits design flaws in the Windows OS, affects all versions of Windows.

The Top 5 Security Threats that Engulfed 2016

Rooting App Rooted in Mobile Environments

In 2016, a number of malicious apps that root Android-based smartphones were discovered. Particularly, from July to October, the number of rooting apps collected by AhnLab increased by 30% compared to the first half of 2016. This shows that the number of malicious apps are constantly increasing.

In the last first half of 2016, the most common malicious apps were those that use root privileges to show ads or surreptitiously install other apps. In the second half of 2016, rooting apps that steal financial information have started to appear. It was confirmed that malicious apps made in China mostly try to acquire root privileges to earn profits by displaying ads or installing apps.

As malicious apps that exploit Android OS vulnerabilities increase, Google is also taking various steps to bolster Android's security. Ever since discovering the Stage Fright vulnerability in 2015, monthly security updates for Android OS have been made available, and the update order of smartphone manufacturers is made public. Android OS v7.0 (Nougat), released in 2016, prohibits to boot after system modulation attempts via rooting. The problem is that there are some cases in which security updates are not supplied depending on the smartphone manufacturer or production year of the terminal.

Top 5 Security Threats that Will Sweep Over 2017

Top 5 Security Threats that Will Sweep Over 2017

Remarkable Security Trends in 2017

AhnLab

Top 5 Security Threats that Will Sweep Over 2017

Changes in Ransomware Targets

Ransomware that spread widely over the past year has become a useful criminal tool for gaining money from an attacker's point of view. For corporations in particular, there have been cases of ransom payments being made since corporations felt risk of interrupting business or losing important data, such as customer information. With the creation and distribution of Ransomware as a Service (RaaS), ransomware has become a market unto itself with both consumers and suppliers.

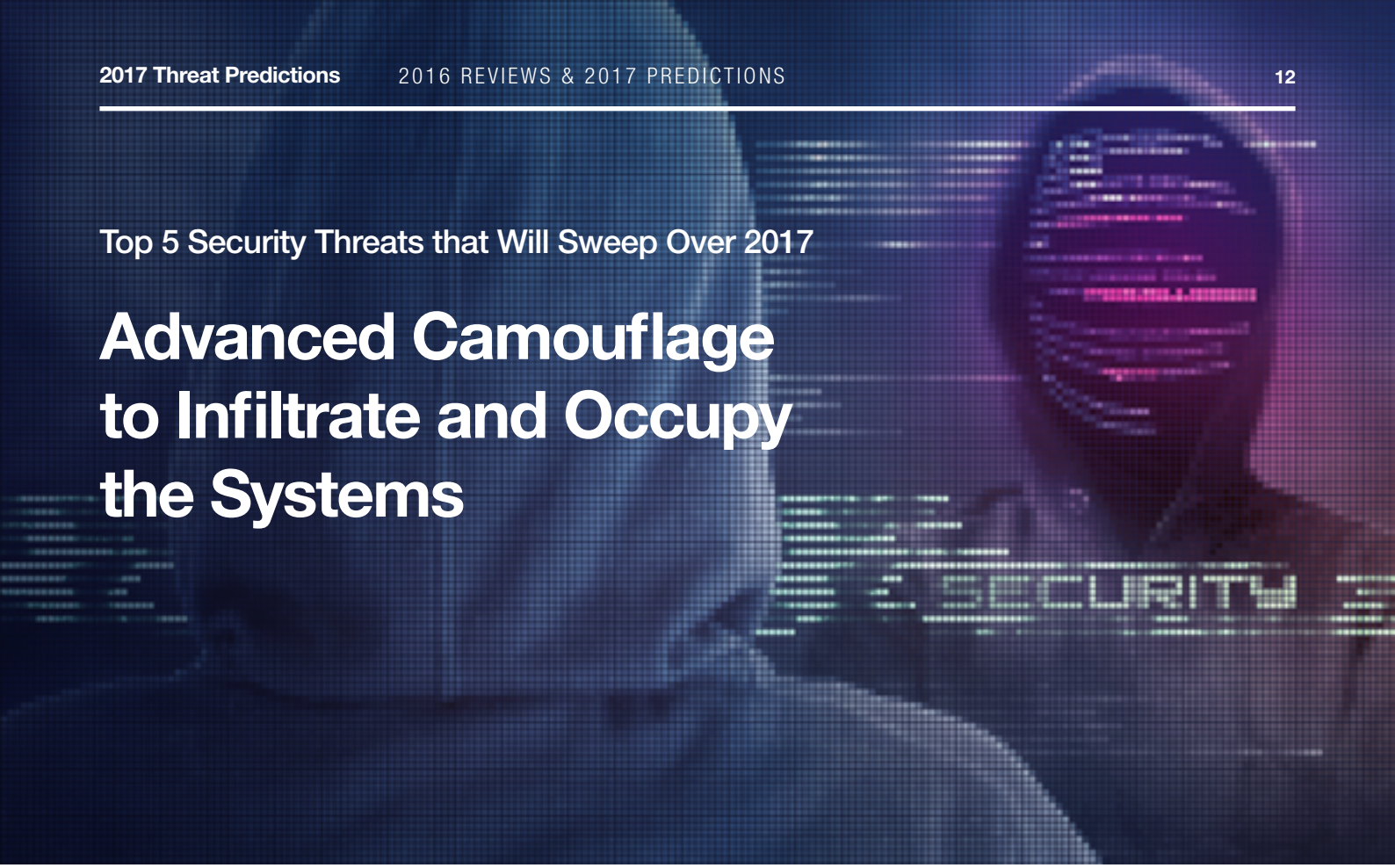
Ransomware threats are expected to increase in frequency and range of attacks this year. With the goal being to acquire money, it is only natural that attackers will target points where money flows. So far now, phishing and pharming scams have mainly took lead financial cybercrimes, but now ransomware is expected to become a mainstream of financial cybercrimes. Also, ransomware has combined with spear phishing and other cybercrime campaigns that target foreign trade transactions and companies.

Top 5 Security Threats that Will Sweep Over 2017

Generalization of Cyberattacks Toolkits

Not so long ago, it was considered that cyberattacks were committed by IT experts and hackers or hacking groups. Nowadays, however, it is possible to generate malware or launch cyberattacks without any IT knowledges and skills since it has become easier to find malware tool kits and a variety of cyberattack services such as RaaS (Ransomware as a Service) and spam mail delivery services not only from the he cyber black market but also via public internet. The generalization of cyberattacks is expected to be exploited for more crimes; it becomes more difficult to specify and investigate who is behind the cybercrimes.

Attackers will continue to use drive-by download method that malware is automatically installed when visiting a website or viewing an e-mail message. Also, attackers will enhance attack techniques, such as exploiting software security vulnerabilities more actively against users who do not promptly apply software security patches. In order to prevent these exploit-based attacks, corporate security managers should regularly check websites and pay extra attention to attacks via web shells.



Top 5 Security Threats that Will Sweep Over 2017

Advanced Camouflage to Infiltrate and Occupy the Systems

Until 2010, most hackings against corporations were committed to steal confidential business data or customer information. Recently, however, the purpose of cyberattacks against corporations has shifted to attempts to infiltrate and take control of corporate internal infrastructure. These types of attacks combine with multiple techniques to penetrate companies and organizations successfully.

The attackers acquire system account by collecting information from employees within the company and then escalate their access to the corporate infrastructure by exploiting infected systems. They then keep searching and collecting various accounts until they finally obtain the privileges to take control the entire systems.

When attackers successfully take over the systems, they are able to use the company's infrastructure as an attack base for large-scale attack: they can distribute malware disguised as normal programs required for accessing the company's services, which users must download and install on their personal computers. These infected computers also can be used for attacks against other corporate systems; that is why this type of attacks are not likely to be discontinued this year.

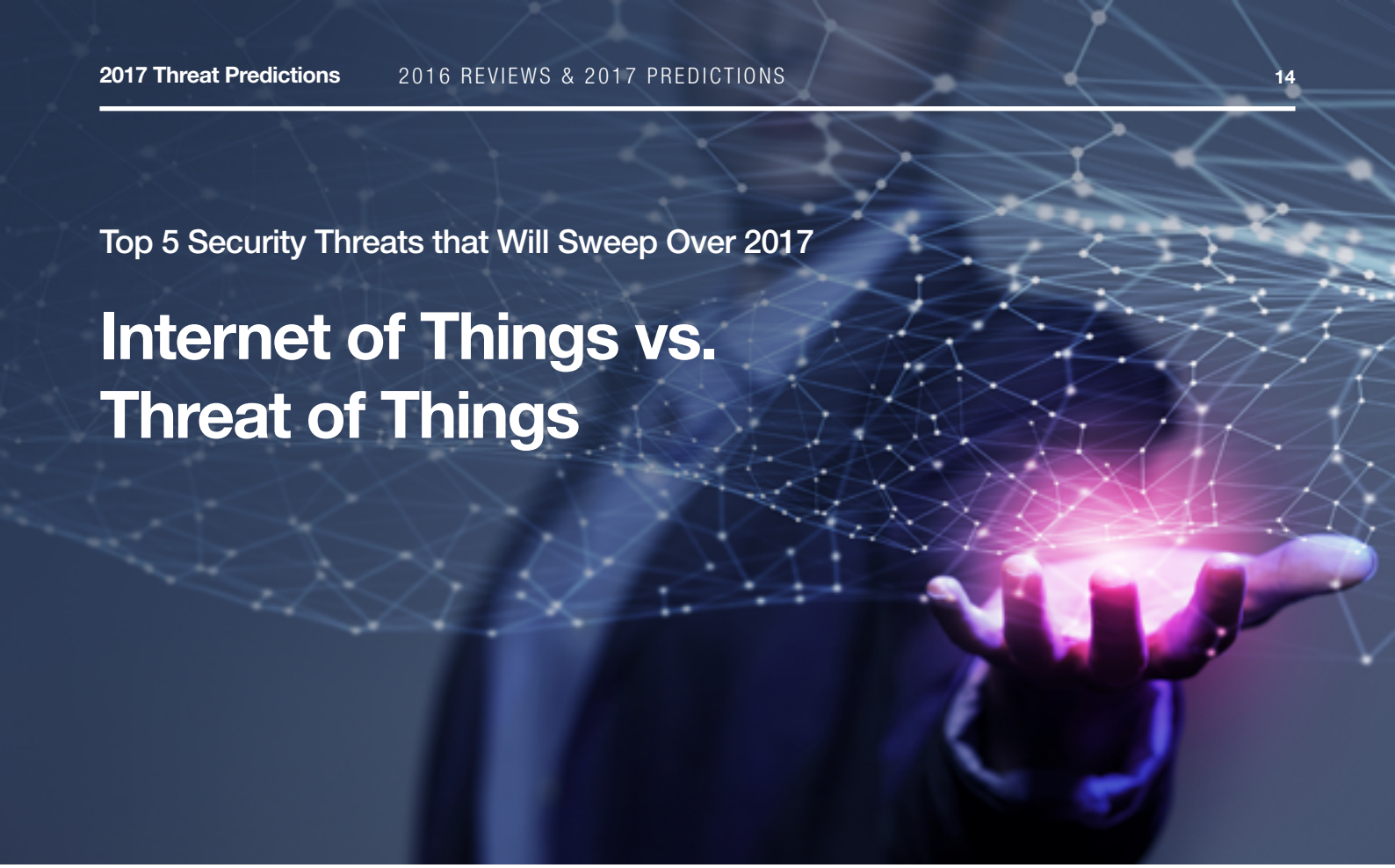
Top 5 Security Threats that Will Sweep Over 2017

Unremitting Cyberattacks against Social Infrastructure

The political and economic conflicts over the world will be more intensified this year; ideological conflicts between nations will be deepen. In other words, cyber terrorism that targets foreign organizations will not halt.

Along with online services used by citizens, the latest cyberattacks target nearly every type of company and organization regardless of service type or size. It is presumed that there are primarily terrorist organizations or hostile countries behind the most cyber terrorism, such as attacks on social infrastructures. Motivations for these types of attacks can also be found in religious, ideological, and political conflicts, in addition to monetary motives. If attacks against social infrastructures succeed, it can maximize the effects of propaganda by causing social confusion and fear. Since it is never easy to resolve religious and political conflicts, these types of attacks continue to increase.

Most systems in social infrastructures are separated from network and are not directly connected to the external Internet. However, if there is even one system connected to the Internet or there is any point connecting the Internet and the internal network, no body can say that they are completely free from security threats. No matter how the systems are protected, the most vulnerable point is always the human; there can be an employee who violates security policies by mistake or other reasons, simply because of inconvenience. Attackers have always keep that it mind and continue targeting human error using various methods to exploit these kinds of vulnerabilities.



Top 5 Security Threats that Will Sweep Over 2017

Internet of Things vs. Threat of Things

The development and proliferation of Internet of Things (IoT) technologies will be accelerated this year; so the IoT security threats do. Due to the lack of IoT device manufacturers' security awareness, the IoT devices with security vulnerabilities continue to be sold. The attackers will never miss the chance; malware target IoT devices will rapidly increase this year.

Once IoT devices are sold or installed, they are used as-is for many years, and thus it is difficult to manage security status. In addition, most IoT device manufacturers can't afford to address security problems due to the lack of funds or technologies. Meanwhile, it is difficult to raise the prices for security enhancement considering the low power and low cost are the main factor for users.

Therefore, it is necessary to foster cooperation between security companies, government agencies, and manufacturers to prevent security threats related to the fast-growing IoT device market. In addition, as various countries rush to develop IoT technology and products competitively, it is difficult to solve a wide range of security threats caused by IoT devices through current regulations. It is imperative to establish a minimum inspection system for IoT devices and to prepare practical guidelines for strengthening security measures through multinational cooperation between governments, industry associations, and manufacturers worldwide.

Advices to Combat Security Threats in 2017

Remarkable Security Trends in 2017

Malware creation and distribution services have become a main part of the cyber black market, and new crime ecosystems are being developed based on this. According to economic principles, this ecosystem will produce more varieties of malware and expand its territory through vigorous activity. Investments and efforts will be continued to create and distribute differentiated malware according to the market logic of capitalistic competition, which will further heighten the security threat this year.

In accordance with the changes of threat landscape, corporations and organizations seem to change their way to approach to security response: there are needs of integrated management for point security solutions and events. Also, security vendors have adopted various new technologies, such as automation and machine learning, in order to process the huge amount of collected information effectively and defeat the latest threats.

Advices to Combat Security Threats in 2017

Trend 1
Machine learning at the center of the security area

Data mining and machine learning technologies to analyze a wide variety of data have emerged; these technologies will become key factors of security area this year. As many point solutions have been deployed for various security issues, complexity of security management has increased in accordance with qualitative and quantitative limits in terms of the manpower to manage the security systems.

There will be various attempts to replace security response from manpower to automation applying new technologies. This will also contribute to finding new insights from information that has been collected via the existing security solutions but regarded as insignificant or overlooked. By combining existing security techniques with new technologies such as machine learning, there will be able to find meaningful results that are worthy of security analysts. At the same time, the resources will be saved by introducing these technologies so that corporations and organizations will be able to afford to focus on or expand business.

Advices to Combat Security Threats in 2017

Trend 2
Security segmentation and integrated management for response

Changes in the era of IT represented by IoT and the cloud, security issues will increase and be segmented for various platforms and services. Companies that have acquired understandings of the latest technology through various research and experiences are applying the appropriate technologies and services for their particular industries.

This should be accompanied by a review of security issues, therefore corporations and organizations will search and select appropriate security technologies and solutions for their environment in this year. In particular, there will be a need for integrated management to monitor and practically and effectively respond to security issues. In addition, visualization of threat information will be the key to effectively and practically respond to identified threats.

Advices to Combat Security Threats in 2017

Trend 3. Blurred lines between 'the wrong' and 'the malicious'

Now, it becomes hard to narrow the suspects who generate malware or launch cyberattacks because it has become easier for people to find malware tool kits and a variety of cyberattack services such as RaaS (Ransomware as a Service) and spam mail delivery services not only from the cyber black market but also via public internet. In addition, exploit kits that use software vulnerabilities and execute malware continue to be upgraded, and cybercrimes caused by exploitation will continuously increase.

The generalization of malware creation and distribution services has made it impossible to specify attackers as limited to specific types of people or specific groups. In other words, security response and investigation of the attackers will face many challenges. In order to minimize exposure to exploit attacks, therefore, it is necessary to raise security awareness for users about the importance of security patches. For companies and organizations, it is necessary to invest for security solutions deployments to reinforce and effectively manage security patches for employees.

Advices to Combat Security Threats in 2017

Conclusion: Security comes down to "human"

Most security breaches in recent years are target attacks that penetrated specific individuals or groups within an organization to achieve a specific purpose. Attack techniques include spear phishing that sends email to specific people or groups and watering holes that hack websites used by a targeted group to distribute malware.

What should be noted in a series of recent security incidents is that the target attacks also start with a malware infiltration and usually feature a poorly-managed PC or server that serves as a bridge to other systems and infrastructure. It is also necessary to build various solutions or use specialized services to prevent security threats in advance, but it is equally important to educate personnel how to operate them and to enforce security rules.

The lackadaisical attitude of security managers as well as employees may result in significant security incidents. Considering that attackers keep their eyes on the most well-known security hole - people -, corporations and organizations are required to educating and managing personnel along with deploying and managing multiple security solutions and services. In order to mitigate damages caused by the ever-evolving threats, the continuous efforts of all the members of corporations and organizations - from end users to security managers and executives- should be made.

Security Trend

2016 REVIEWS &
2017 PREDICTIONS

Publisher AhnLab, Inc.
Contributors ASEC Researchers
Editor Content Creatives Team

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel. +82 31 722 8000 | Fax. +82 31 722 8901

AhnLab.com

AhnLab

Security Trend

2016 REVIEWS &
2017 PREDICTIONS

AhnLab