Security Trend

ASEC REPORT

VOL.70

October, 2015

AhnLab

ASEC REPORT

VOL.70 October, 2015

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This monthly report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

SECURITY TREND OF OCTOBER 2015

Table of Contents

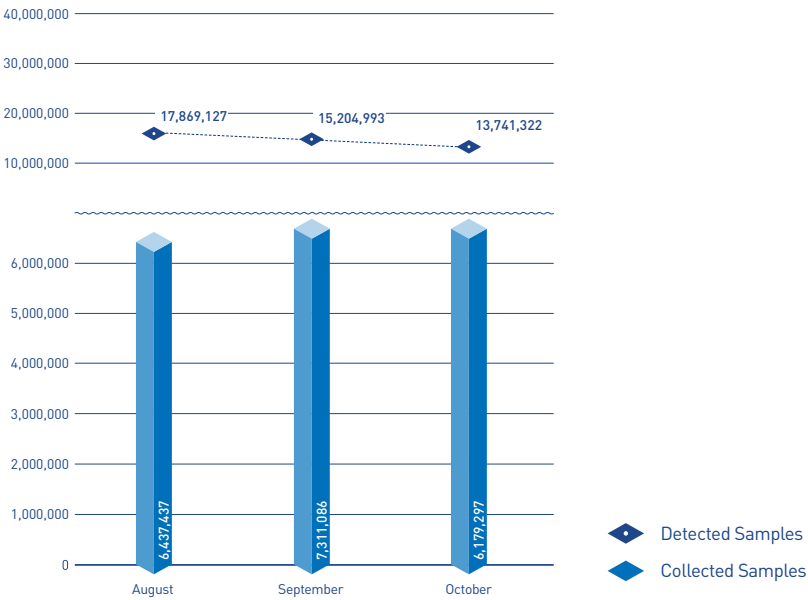
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

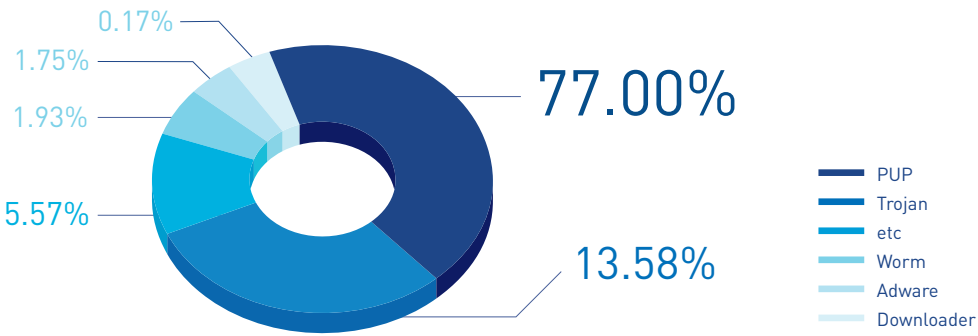
According to the ASEC (AhnLab Security Emergency Response Center), 13,741,322 malware were detected in October 2015. The number of detected malware decreased by 1,463,671 from 15,204,993 detected in the previous month as shown in Figure 1-1. A total of 6,179,297 malware samples were collected in October.



[Figure 1-1] Malware Trend

* "Detected Samples" refers to the number of malware detected by AhnLab products deployed by our customers.
* "Collected Samples" refers to the number of malware samples collected autonomously by AhnLab that were besides our products.

Figure 1-2 shows the prolific types of malware in October 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 77% of the total. It was followed by Trojan (13.58%) and Adware (1.93%).



[Figure 1-2] Proportion of Malware Type in October 2015

Table 1-1 shows the Top 10 malware threats in October categorized by alias. Trojan/Win32.Starter was the most frequently detected malware (129,910), followed by Trojan/Win32.Gen (114,801).

[Table 1-1] Top 10 Malware Threats in October 2015 (by Alias)

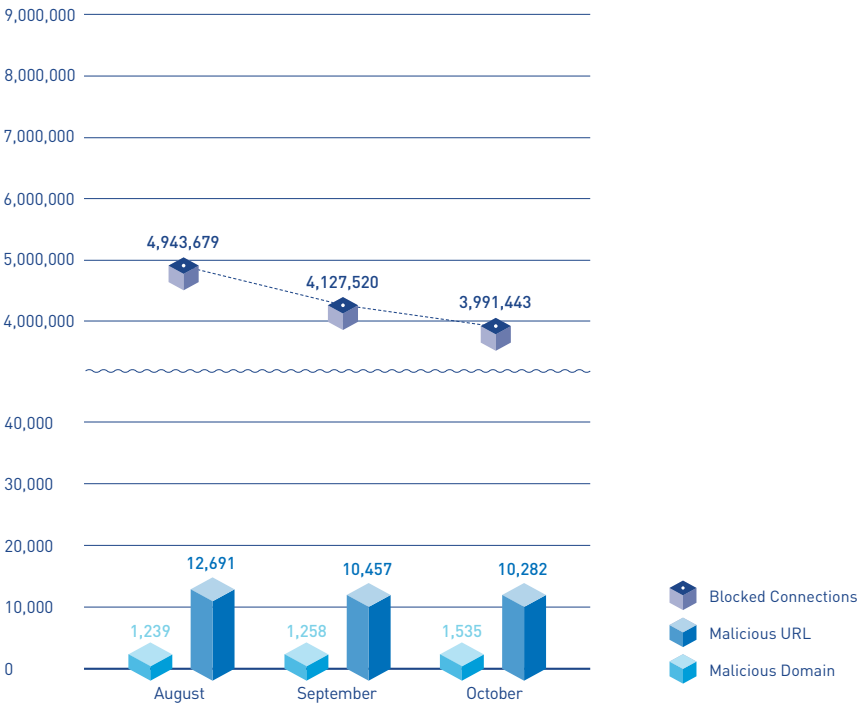
Rank	Alias from AhnLab	No. of detections
1	Trojan/Win32.Starter	129,910
2	Trojan/Win32.Gen	114,801
3	Trojan/Win32.Agent	103,522
4	Malware/Win32.Generic	98,757
5	Trojan/Win32.Banki	80,456
6	Trojan/Win32.OnlineGameHack	60,435
7	Unwanted/Win32.Exploit	53,141
8	Worm/Win32.IRCBot	46,705
9	Unwanted/Win32.Keygen	46,642
10	Trojan/Win32.Generic	45,917

SECURITY STATISTICS

02

Web Security Statistics

In October 2015, a total of 1,535 domains and 10,282 URLs were comprised and used to distribute malware. In addition, 3,991,443 malicious domains and URLs were blocked.



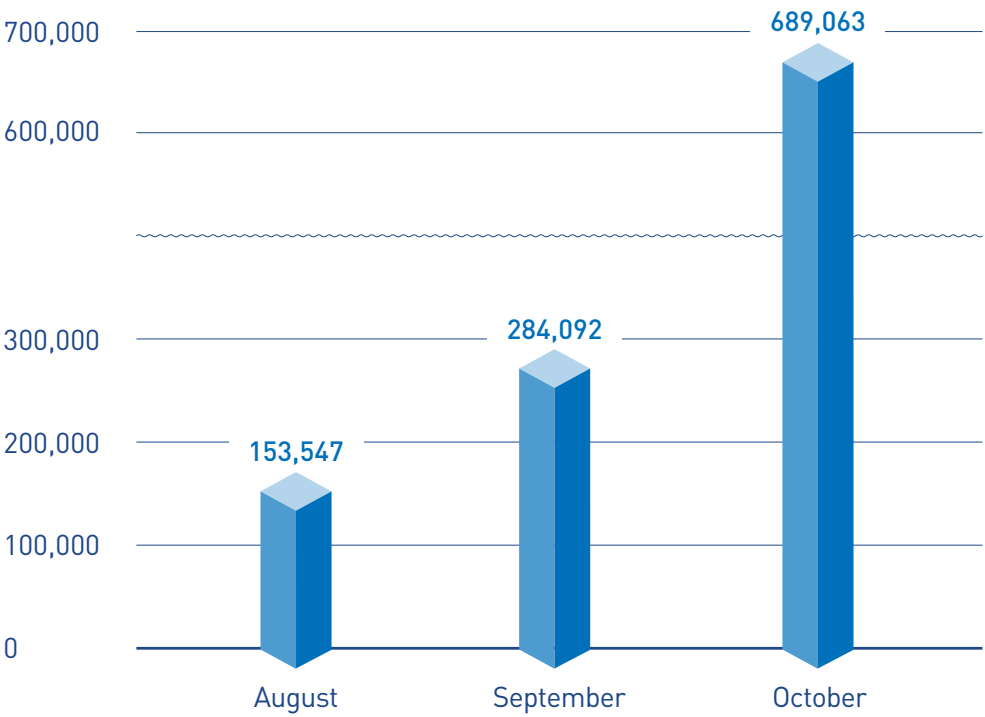
[Figure 1-3] Blocked Malicious Domains/URLs in October 2015

* "Blocked Connections" refers to the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers.

SECURITY STATISTICS

03 Mobile Malware Statistics

In October 2015, 689,063 mobile malware were detected as shown in Figure 1-4.



[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in October 2015. Android-PUP/SmsPay was the most distributed malware with 330,240 of the total.

[Table 1-2] Top 10 Mobile Malware Threats in October (by alias)

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	330,240
2	Android-Trojan/FakeInst	56,645
3	Android-PUP/SmsReg	34,608
4	Android-PUP/Noico	29,980
5	Android-PUP/Dowgin	21,709
6	Android-PUP/Zdpay	21,324
7	Android-PUP/Downloader	20,501
8	Android-Trojan/Opfake	16,596
9	Android-PUP/Mmsreg	15,523
10	Android-Trojan/Opfake	11,645

2

SECURITY ISSUE

Phishing Scam Disguised as "Blue Screen"

SECURITY ISSUE

Phishing Scam Disguised as "Blue Screen"

Long-time users of Windows are no doubt familiar with the blue splash screen and white text that displays error messages for the operating system. It is called as "Blue Screen of Death," or BSOD in short, for the way it suddenly appears to wreak havoc. A recent malicious site has been discovered that disguises itself as the blue screen error display. The site is a phishing scam designed to deceive users and extort money.

Figure 2-1 | Malicious site disguised as a "blue screen" display

Figure 2-1 shows the recently-discovered phishing site disguised as the Blue Screen. It states, "Windows health is critical/do not restart/please contact Microsoft technicians." A toll-free number is provided, and when the user calls the number a scammer posing as a Microsoft employee demands payment in order to restore the system.

The Windows Blue Screen is used by certain versions of the operating system to indicate a critical and unrecoverable error, such as memory access violation or hardware and software errors. The screen is a type of an error message that indicates the cause of the Windows error, but its unexpected appearance and overpowering blue presence is strong enough to rattle most users. Many people have no doubt experiencing the despair of a sudden splash of blue across their screen interrupting their unsaved work. The newly-discovered phishing site takes advantage of this feeling of unsettlement felt by users.

Skilled computer users, of course, will quickly realize that the screen as shown in Figure 2-1 is not a real Blue Screen. However, this phishing site includes a script that blocks user-directed events in the source code of the Web page, as shown in Figure 2-2, preventing the internet browser from being shut down unless the user manually ends the process through Windows Task Manager. For this reason, many users may be too surprised to realize that it is a fake display.

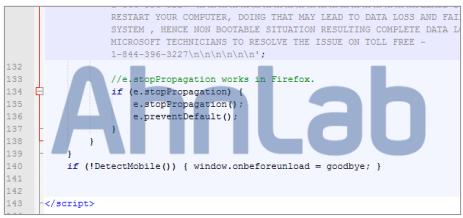


Figure 2-2 | HTML source code of the malicious site

This phishing site was confirmed to have used Google advertising links to randomly deceive users into accessing the site. The malicious site uses ad links that are displayed on the top of the search results page when the user searches for certain key words.

A query using the same IP address for just several days shows the following URLs being used.

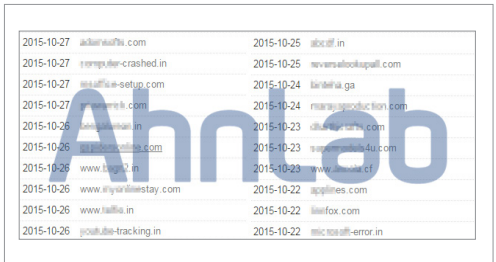


Figure 2-3 | List of URLs using the same IP address

This issue has been reported to Google and the links of the phishing sites have been deleted. However, the attackers continue to distribute the site by changing one or two letters in the URL, requiring extra vigilance on the part of the users.

3

IN-DEPTH ANALYSIS

Malware Distributed via PDF Files on the Rise

SECURITY ISSUE

Malware Distributed via PDF Files on the Rise

Multiple attacks using malicious PDF files have been recently reported. These malicious files are often distributed by being disguised as work-related email attachments, requiring extra care by businesses. ASEC Report Vol. 70 examines how PDF malware are distributed and outlines preventive measures by highlighting two recent cases.

■ **Case 1: Banki malware using PDFs**

A user received an email from the sales representative of a vendor. The email subject appeared to indicate that it contains an updated price list for the current month. Accustomed to receiving such emails monthly, he opens the PDF attachment without a second thought. The PDF file, however, only contains two letters ("dd"), and a pop-up window appears asking him to open the attachment. Wondering whether the file format of the attachment has been changed without his knowledge, he presses the "OK" button on the pop-up window. Then Microsoft Word opens and a document is loaded, but again without any content. An error message appears on the top of the documents, something to the effect of "Cannot run the macro...." Frustrated at the hoops he is being forced to go through, he clicks the macro, again to no visible effect. Irritated, he decides that he will make a phone call to the company later to figure out what is going on, closes Word, and goes back to his work.

That afternoon, he logs onto an internet banking site to transfer funds to another company, and is met by a pop-up window that prompts him to enter his entire bank security card code. Something does not seem right.

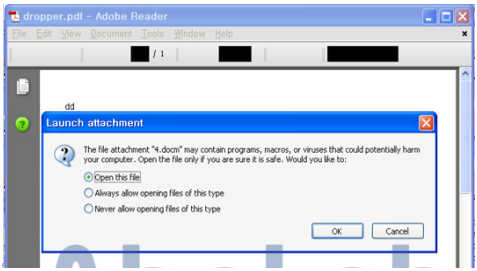


Figure 3-1 | A malicious PDF file that contains another document file and an .exe file inside

The case cited above is a reconstruction of an attack when the email account of the sales representative is compromised and malicious PDF files are sent as email attachments to everyone on the contact list. Fortunately, some suspicious indicators can be found in the case above. The empty PDF document is a curiosity, but clear signs that something is amiss include the fact that an MS Word document was embedded in the PDF file, and that the Word file again had no text but included a macro. However, average users or even users with some knowledge of computers would be hard pressed to spot such suspicious signs in most kinds of attacks.

▶Findings 1: Attack tactics

First, a tool was used to parse through the PDF file attachment of the email to search for certain key strings. The tool discovered the presence of JavaScript in the PDF file, and an embedded file.

Figure 3-2 | Searching for key strings in the PDF file

The embedded file is suspicious, but the JavaScript code could be normal. Let us then examine what the JavaScript code functions, and the type of file embedded in the email attachment. Figure 3-3 is the header of file embedded in the PDF file, and file formats that have PK or 50 4B as file headers include ZIP, KARs, MS Office and Open Documents files.

Figure 3-3 | File headers in the embedded file

Noting that the name of the file shows in the pop-up window in Figure 3-1 earlier was "4.docm," it can be deduced that the file embedded in the PDF attachment is an MS Office document file with a macro.

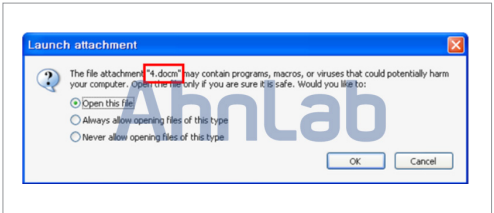


Figure 3-4 | Detailed biew of the pop-up window in [3-1]

The JavaScript code inserted into the PDF file is a command for extracting and executing a certain object, in this case designed to extract the DOCM file in the PDF file into a temp folder and execute it.

Figure 3-5 | JavaScript code in the PDF file

Let us now examine what the DOCM file in the PDF file executed by the JavaScript code does. Figure 3-6 shows the OLE data stream in the file "4.docm" converted into string. The "ceece.exe" file is downloaded and executed by using a macro in stream A3.

Figure 3-6 | The exe file being run by the macro

The "ceece.exe" file was identified to be a Banki malware often used in pharming attacks. The download path for this file as discovered in stream A3 is shown below:

http://kons****au.re****ika.pl/07jhnb4/0kn7b6gf.exe

▶Findings 2: Preventing attacks via malicious PDF files

The malicious PDF itself can be blocked by using the "Trust Manager" function of Adobe PDF Reader. The user can uncheck the "Allow opening of non-PDF file attachments with external applications" option under [Edit] > [Preferences] > [Trust Manager].

Keeping this option disabled can prevent a file embedded in a PDF file being executed without the user being prompted.

For businesses with a large number of users, it can be an effective way to distribute the following registry values through "active directory."

[Registry Setting Guide]

- Path: HKLM₩SOFTWARE₩Policies₩Adobe₩<product name>₩<version>₩FeatureLockDown₩cDefaultLaunchAttachmentPerms
- Registry name: tBuiltInPermList
- Registry value:

version:1|.ade:3|.adp:3|.app:3|.arc:3|.arj:3|.asp:3|.bas:3|.bat:3|.bz:3|.bz2:3|.cab:3|.chm:3|.class:3|.cmd:3|.com:3|.command:3|.cpl:3|.crt:3|.csh:3|.desktop:3|.dll:3|.exe:3|.fxp:3|.gz:3|.hex:3|.hlp:3|.hqx:3|.hta:3|.inf:3|.ini:3|.ins:3|.isp:3|.its:3|.job:3|.js:3|.jse:3|.ksh:3|.lnk:3|.lzh:3|.mad:3|.maf:3|.mag:3|.mam:3|.maq:3|.mar:3|.mas:3|.mat:3|.mau:3|.mav:3|.maw:3|.mda:3|.mdb:3|.mde:3|.mdt:3|.mdw:3|.mdz:3|.msc:3|.msi:3|.msp:3|.mst:3|.ocx:3|.ops:3|.pcd:3|.pi:3|.pif:3|.prf:3|.prg:3|.pst:3|.rar:3|.reg:3|.scf:3|.scr:3|.sct:3|.sea:3|.shb:3|.shs:3|.sit:3|.tar:3|.taz:3|.tgz:3|.tmp:3|.url:3|.vb:3|.vbe:3|.vbs:3|.vsmacros:3|.vss:3|.vst:3|.vsw:3|.webloc:3|.ws:3|.wsc:3|.wsf:3|.wsh:3|.z:3|.zip:3|.zlo:3|.zoo:3|.pdf:2|.fdf:2|.jar:3|.pkg:3|.tool:3|.term:3

However, it should be carefully considered since disabling the "Allow opening of non-PDF file attachments with external applications" via the Adobe Reader menu will generate values that include a large number of different file formats.

■ Case 2: Phishing using PDF files

"Phishing" is a portmanteau of the words "private data" and "fishing," a method of attack that disguises itself as a well-known company or agency that the user trusts to lure users into entering their private information. A recently discovered case uses a PDF file that is disguised as an invoice sent by a shipping company to trick the user into accessing a phishing site.

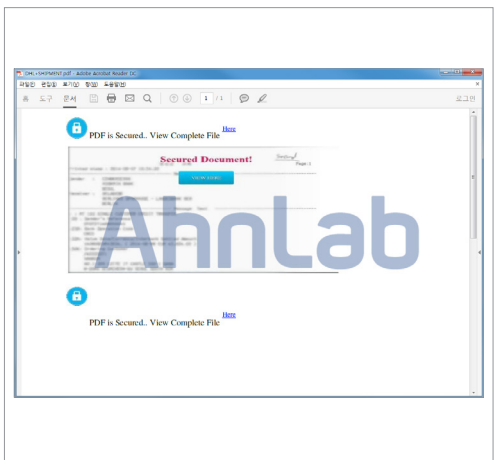


Figure 3-7 | PDF display when executed

The PDF file is disguised to have originated from a well-known shipping company, and a message is displayed saying that the document is encrypted and entices the user into accessing the Phishing web site.

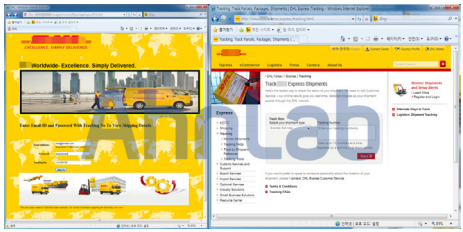


Figure 3-8 | Normal site (left) and Phishing site (right)

Clicking the link in the PDF file sends the user to the Phishing site, which demands an email address, password and tracking number. However, the normal shipping company's web site only asks for the minimum amount of information needed to track the shipment. Users should be cautious of sites that demand excessive personal information.

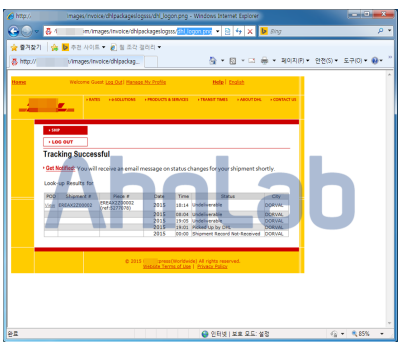


Figure 3-9 | Display once the information has been entered

Entering the required information displays a screen as shown above in Figure 3-9. It displays an image file that is shown regardless of the personal data that has been entered. The information entered by the user is sent to a server that is unrelated to the shipping company. The data is sent unencrypted, as shown in Figure 3-10 below.

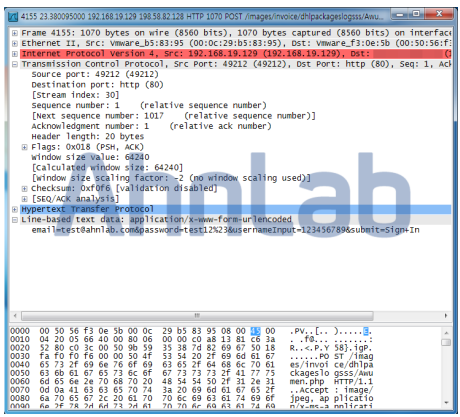


Figure 3-10 | Packet containing the input data

There is another case involving a PDF file that tricks the user into accessing a Phishing site. Clicking the link in this particular PDF displays a message that states, "This document is password protected," as shown in Figure 3-11, and the user's email address and password is demanded.

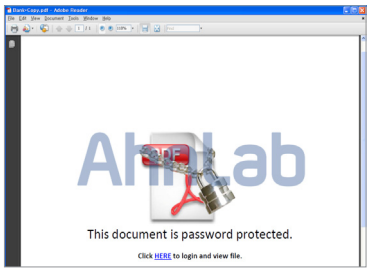


Figure 3-11 | PDF display when executed

Figure 3-12 | Phishing site

Entering the user ID and password and clicking the "View File" button displays a normal document on the browser, and the information that has been entered is compromised.

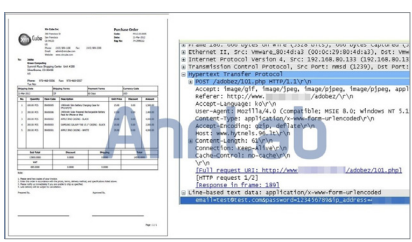


Figure 3-13 | The document that appears after personal data has been entered (left) and the packet containing the information (right)

Personal information leakage can lead to its misuse and additional damage, thus users should be very cautious when opening attachments or clicking on links contained in suspicious emails. Web sites that demand personal information such as passwords or financial information should be considered suspicious, and the companies or agencies should be contacted to ensure that these demands are legitimate.

The corresponding aliases from V3 products, AhnLab's anti-virus program, are as below:

< Aliases from V3 products >

PDF/Fakeinvoice (2015.10.15.00)
PDF/Phish (2015.10.12.08)
W97M/Downloader (2015.08.19.02)
Trojan/Win32.Banker (2015.08.14.00)

AhnLab

ASEC REPORT

VOL.70
October, 2015

Contributors **ASEC Researchers**
Editor **Content Creatives Team**
Design **Design Team**

Publisher **AhnLab, Inc.**
Website **www.ahnlab.com**
Email **global.info@ahnlab.com**