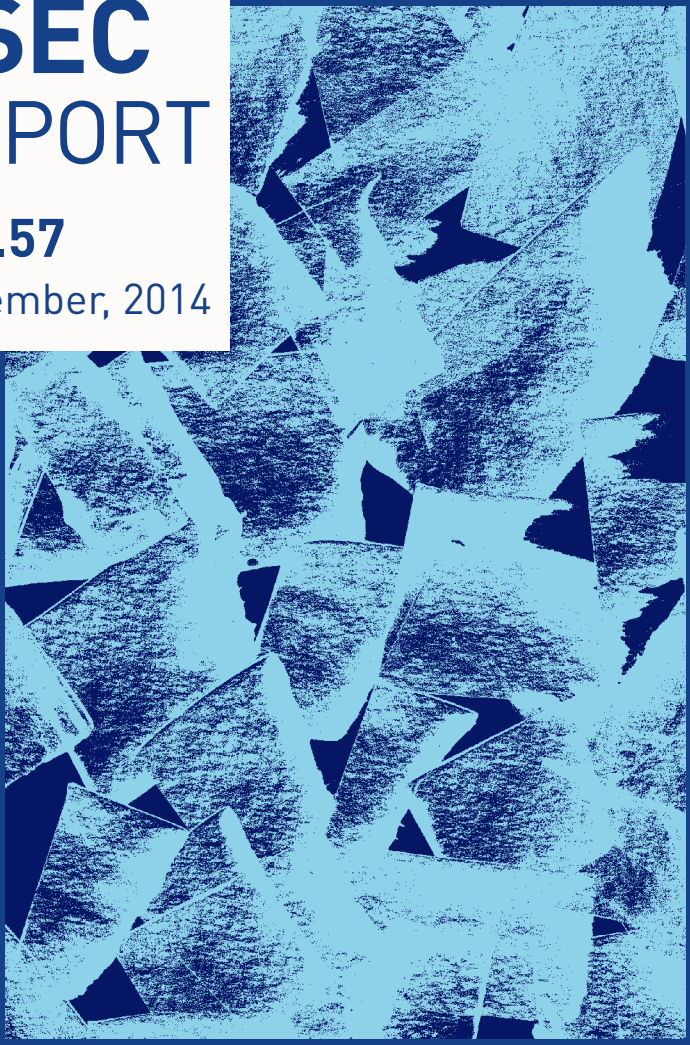
Security Trend

ASEC REPORT

VOL.57

September, 2014



AhnLab

ASEC REPORT

VOL.57 September, 2014

[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 SEPTEMBER 2014

Table of Contents

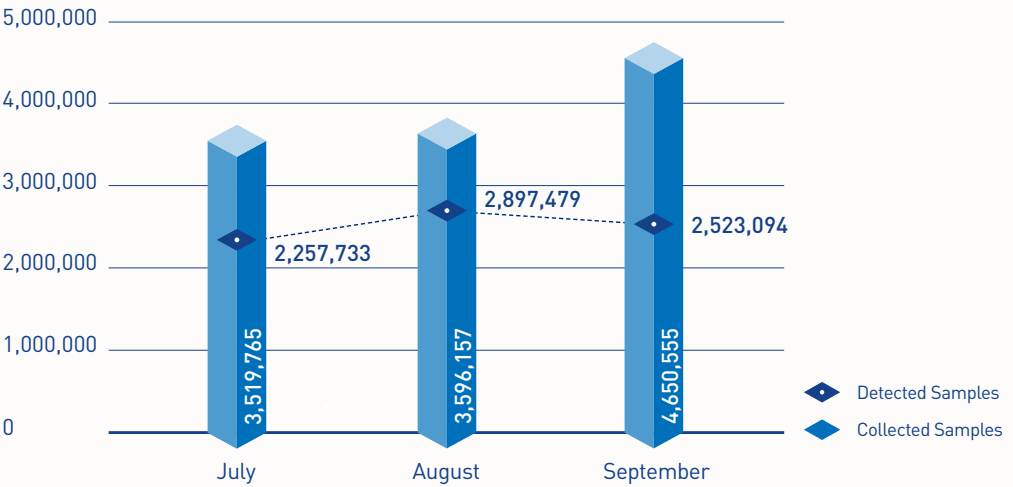
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

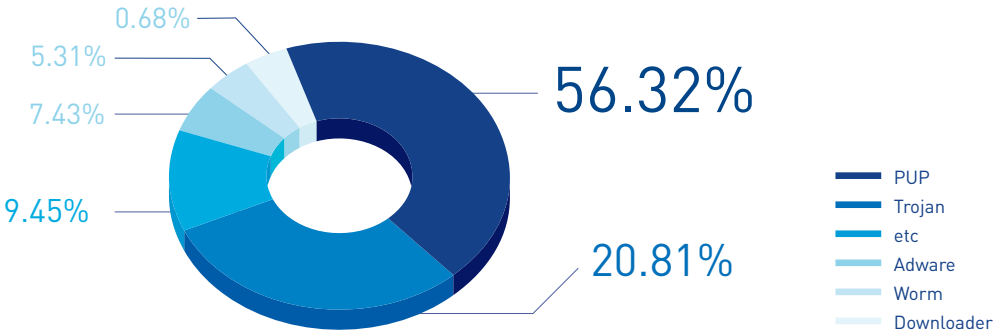
According to the ASEC (AhnLab Security Emergency Response Center), 2,523,094 malware were detected in September 2014. The number of detected malware decreased by 374,385 from 2,897,479 detected in the previous month as shown in Figure 1-1. A total of 4,650,555 malware samples were collected in September.



[Figure 1-1] Malware Trend

In Figure 1-1, "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 September 2014. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 56.32% of the total. It was followed by Trojan (20.81%) and Adware (7.43%).



[Figure 1-2] Proportion of Malware Type in September 2014

Table 1-1 shows the Top 10 malware threats in September categorized by malicious code name. Adware/Win32.SwiftBrowse was the most frequently detected malware (322,808), followed by Adware/Win32.SearchSuite (166,569).

[Table 1-1] Top 10 Malware Threats in September 2014 (by malicious code name)

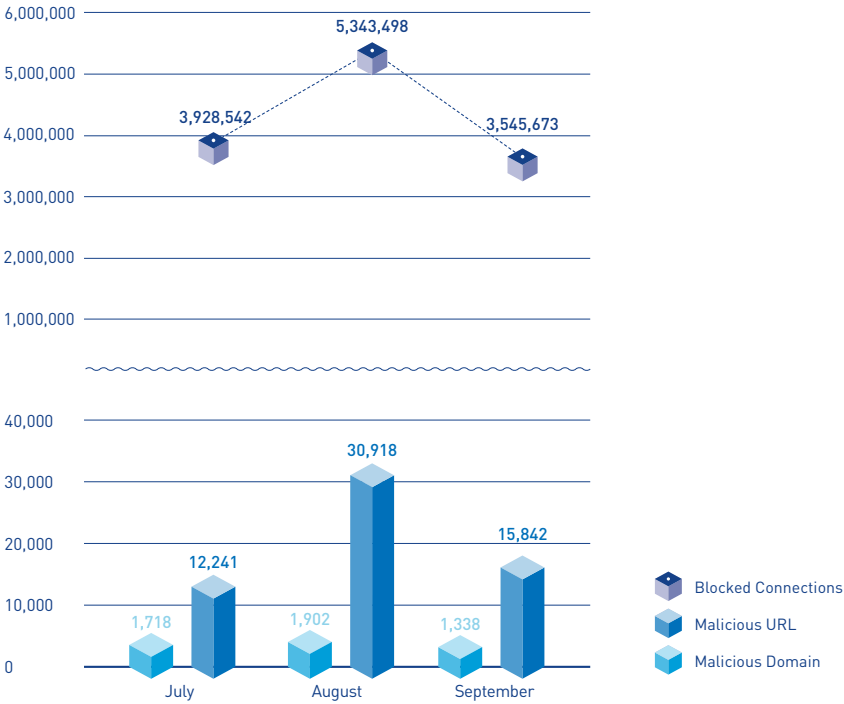
Rank	Malicious code name	No. of detections
1	Adware/Win32.SwiftBrowse	322,808
2	Adware/Win32.SearchSuite	166,569
3	PUP/Win32.SwiftBrowse	102,640
4	Trojan/Win64.SwiftBrowse	86,289
5	Trojan/Win32.OnlineGameHack	84,313
6	Trojan/Win32.Agent	73,619
7	ASD.Prevention	67,765
8	PUP/Win32.IntClient	56,031
9	Malware/Win32.Generic	45,396
10	Adware/Win32.Agent	40,932

SECURITY STATISTICS

02

Web Security Statistics

In September2014, a total of 1,338 domains and 15,842URLs were comprised and used to distribute malware. In addition, 3,545,673 malicious domains and URLs were blocked. This figure is the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers. Finding a large number of distributing malware via websites indicates that internet users need to be more cautious when accessing websites.

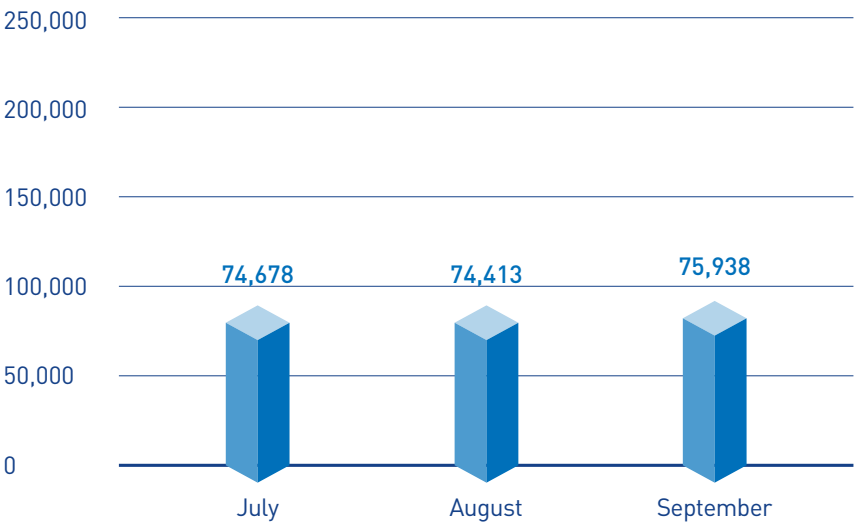


[Figure 1-3] Blocked Malicious Domains/URLs in September 2014

SECURITY STATISTICS

03 Mobile Malware Statistics

In September 2014, 75,938 mobile malware were detected as shown in Figure 1-4.

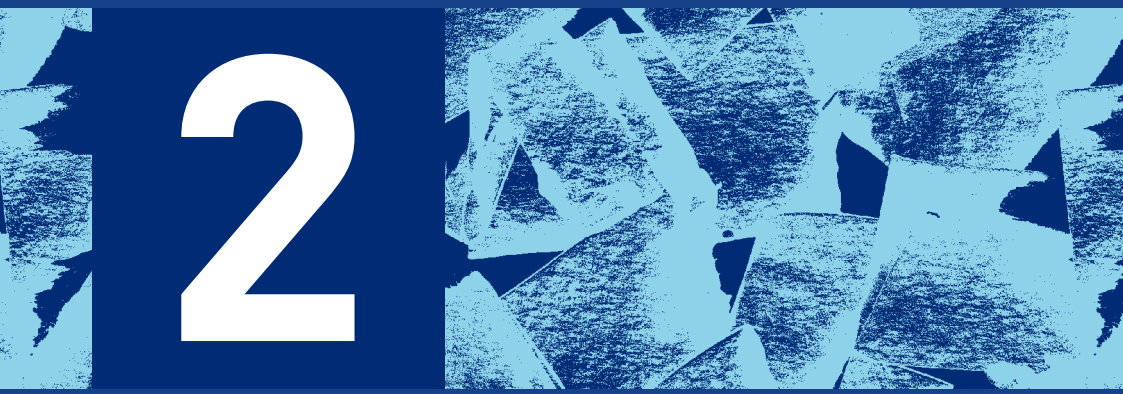


[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in September 2014. On the rise are mobile malware that steal received SMS or secretly send SMS such as Trojan/SmsSend, Android-Trojan/SmsSpy and Android-Trojan/SMSAgent.

[Table 1-2] Top 10 Mobile Malware Threats in September (by malicious code name)

Rank	Malicious code name	No. of detections
1	Android-PUP/Dowgin	18,243
2	Android-Trojan/FakeInst	15,311
3	Android-PUP/SMSReg	5,238
4	Android-Trojan/Opfake	2,409
5	Android-Trojan/SmsSend	1,803
6	Android-Trojan/Agent	1,579
7	Android-Trojan/SMSAgent	1,578
8	Android-PUP/Wapsx	1,460
9	Android-Trojan/SmsSpy	1,308
10	Android-PUP/SMSpay	1,240



2

SECURITY ISSUE

"Am I a Spammer?": Malware to Send Spam E-mails via Users' PCs

"Am I a Spammer?": Malware to Send Spam E-mails via Users' PCs

Your PC could be sending out massive spam e-mails without your knowledge. That could become quite awkward for both you and your receivers. Since the discovery of the malware that loads itself onto a PC's memory and then sends out spam e-mail, users have been urged to be cautious.

Once executed, the malware performs functions restoration to decrypt the PE file which is hidden inside the malware. The restored PE file is then used in the memory through the WriteProcessMemory procedure. The malware copies itself into the path shown in Figure 2-1 and registers it in the registry to execute as the system restarts.

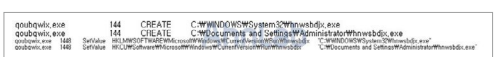


Figure 2-1 | File generation and registry registration

Once the file generation is completed, the second hidden PE file is decrypted again.

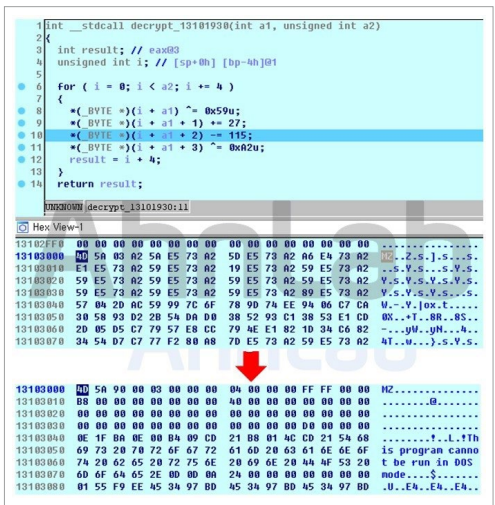


Figure 2-2 | Second PE file decryption

While the first PE file is directly written in the memory, the second PE file is loaded by snchost.exe as shown in Figure 2-3. At this point, the svchost.exe process is generated as a 'suspend format' and the decrypted PE codes are overwritten by functions such as

GetContextThread, ReadProcessMemory, WriteProcessMemory, SetThreadContext, and ResumeThread.

Figure 2-3 | Generation of the svchost.exe process in a suspend format

Through this process, if the execution of the initial malware is terminated, the malicious codes that are written in svchost.exe enable the malicious functions to continue. The malicious codes loaded in svchost.exe communicate with a C&C server to receive commands and generate spam. The packets exchanged in this procedure are encrypted as shown to the left in Figure 2-4, but the corresponding key changes every time.

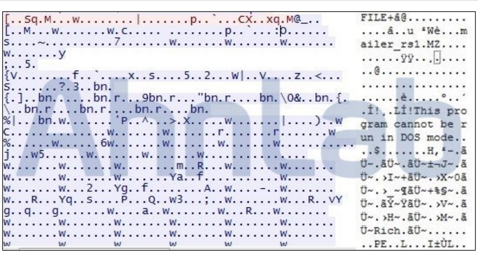
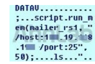
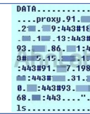
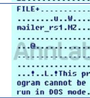


Figure 2-4 | Encrypted packets (left) and decrypted packets (right)

Table 2-1 shows some of the received commands from the C&C server.

Table 2-1 | Commands from the C&C server

Data	Country	
	script (run_file, un_mem, random, random_cmd)	
	Proxy	
File	-	

There are reports that the same symptoms continue to appear on the infected PC even when the corresponding malware has been removed. This is because the malicious codes have been loaded into the memory and then executed; thus, the symptoms can be eliminated by arranging memory such as rebooting the system.

The malware generates tens of thousands of spam emails per day. Therefore, if a PC suddenly generates a large numbers of SMTP packets, the user should be suspicious of malware infection which sends spam emails.

V3, AhnLab's anti-virus product, detects the corresponding malware below:

< Malicious code name in V3 products >

Dropper/Win32.Zbot (2014.09.18.00)

AhnLab

ASEC REPORT

VOL.57
September, 2014

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

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