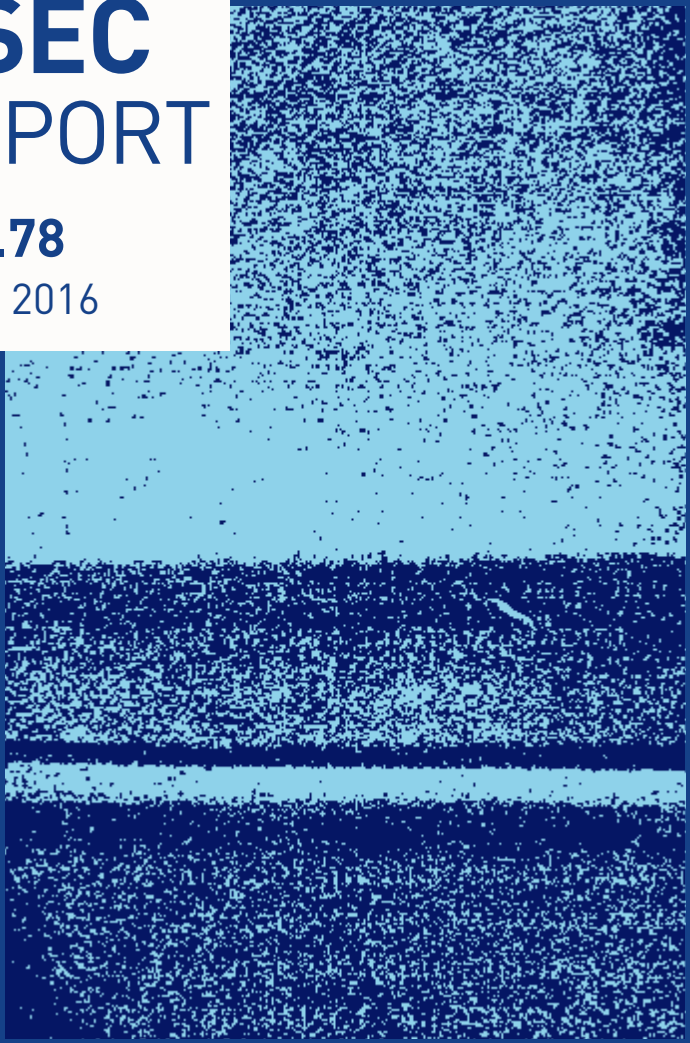
Security Trend

ASEC REPORT

VOL.78

June, 2016



AhnLab

ASEC REPORT

VOL.78 June, 2016

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 June 2016

Table of Contents

1 SECURITY STATISTICS

01 Malware Statistics 4

02 Web Security Statistics 6

03 Mobile Malware Statistics 7

2 SECURITY ISSUE

Cross-platform Adware Appears 10

3 IN-DEPTH ANALYSIS

Ransomware Using "Malvertising" Plague Users 13

1

SECURITY STATISTICS

01 Malware Statistics

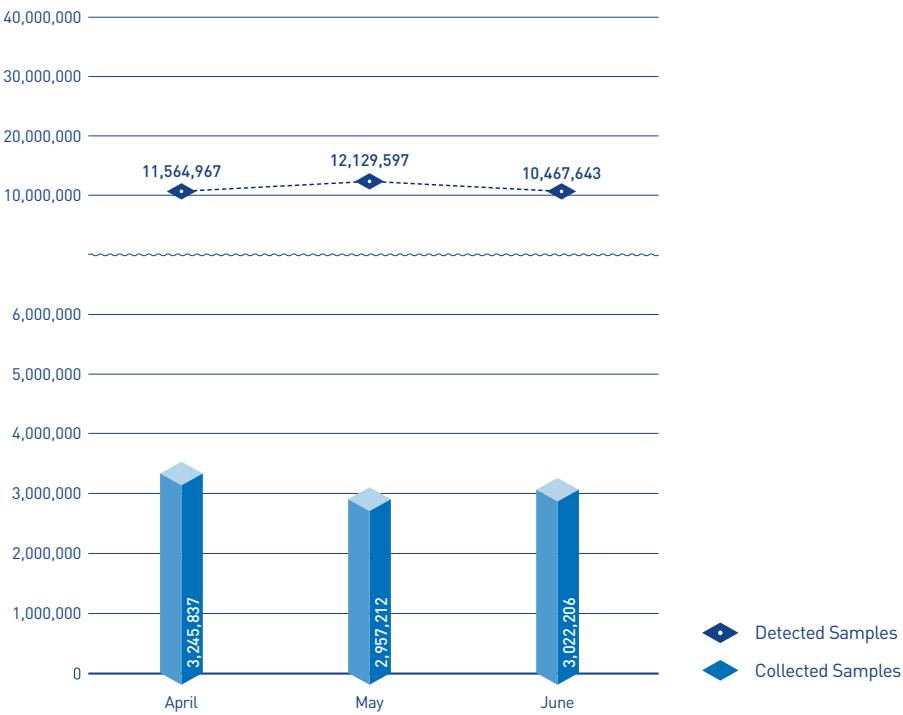
02 Web Security Statistics

03 Mobile Malware Statistics

SECURITY STATISTICS

01
Malware Statistics

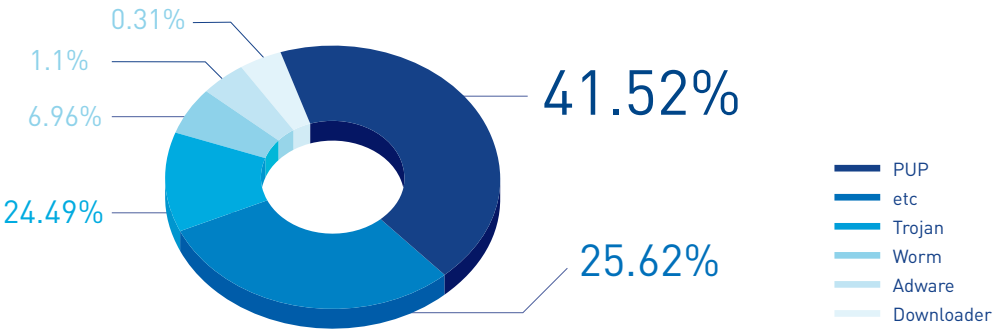
According to the ASEC (AhnLab Security Emergency Response Center), 10,467,643 malware were detected in June 2016. The number of detected malware decreased by 1,661,954 from 12,129,597 detected in the previous month as shown in Figure 1-1. A total of 3,022,206 malware samples were collected in June.



[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 June 2016. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 41.52% of the total. It was followed by Trojan (24.49%) and Worm (6.96%).



[Figure 1-2] Proportion of Malware Type in June 2016

Table 1-1 shows the Top 10 malware threats in June categorized by alias. Trojan/Win32.Starter was the most frequently detected malware (215,746), followed by Malware/Win32.Generic (172,381).

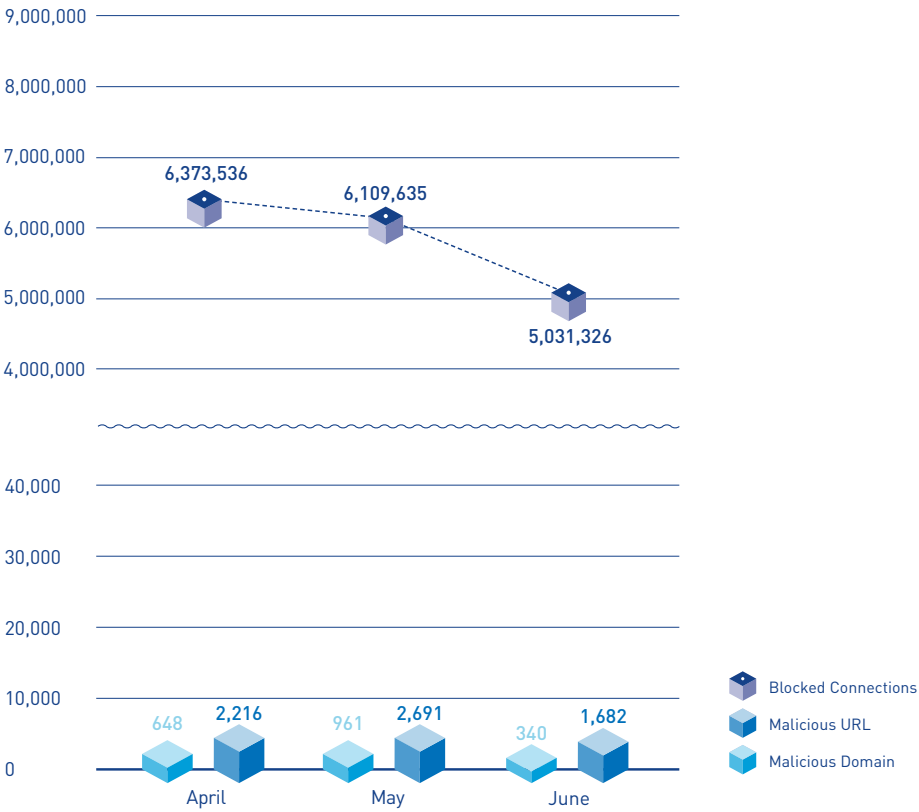
[Table 1-1] Top 10 Malware Threats in June 2016 (by Alias)

Rank	Alias from AhnLab	No. of detections
1	Trojan/Win32.Starter	215,746
2	Malware/Win32.Generic	172,381
3	ASD.Prevention	128,266
4	Unwanted/Win32.HackTool	98,625
5	Trojan/Win32.Agent	73,884
6	Trojan/Win32.Neshta	68,886
7	Trojan/Win32.Banki	68,409
8	Trojan/Win32.CryptXXX	62,640
9	HackTool/Win32.Crack	61,036
10	Unwanted/Win32.Keygen	53,875

SECURITY STATISTICS

02
Web Security Statistics

In June 2016, a total of 340 domains and 1,682 URLs were comprised and used to distribute malware. In addition, 5,031,326 malicious domains and URLs were blocked.



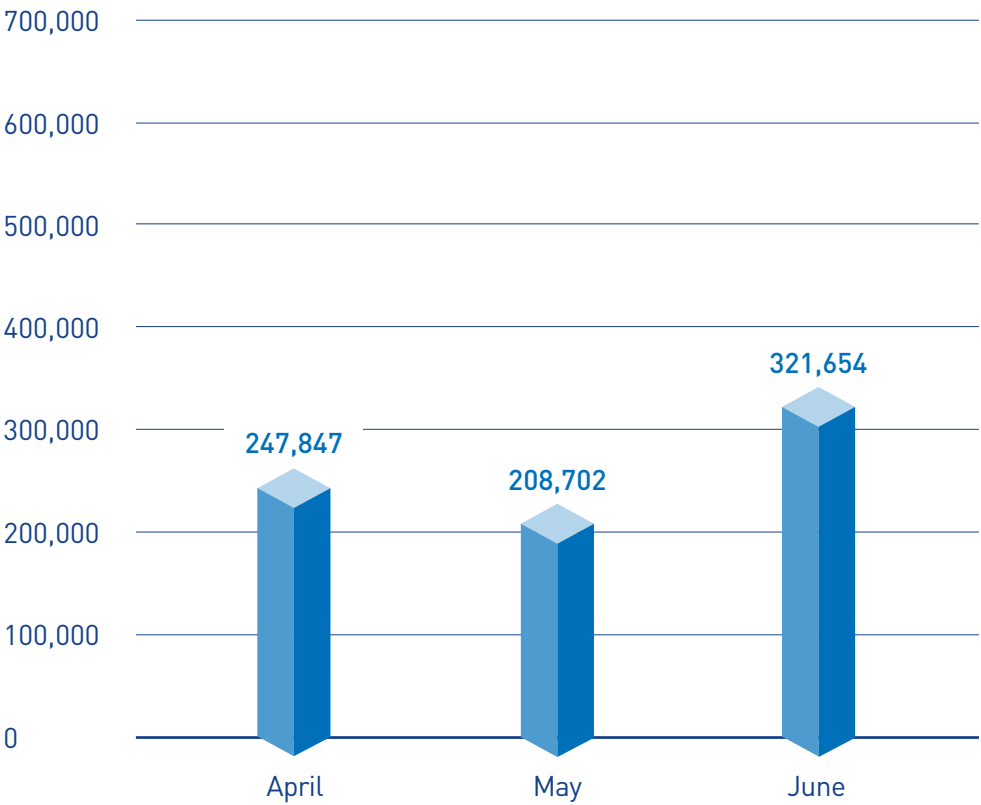
[Figure 1-3] Blocked Malicious Domains/URLs in June 2016

* "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 June 2016, 321,654 mobile malware were detected as shown in Figure 1-4.

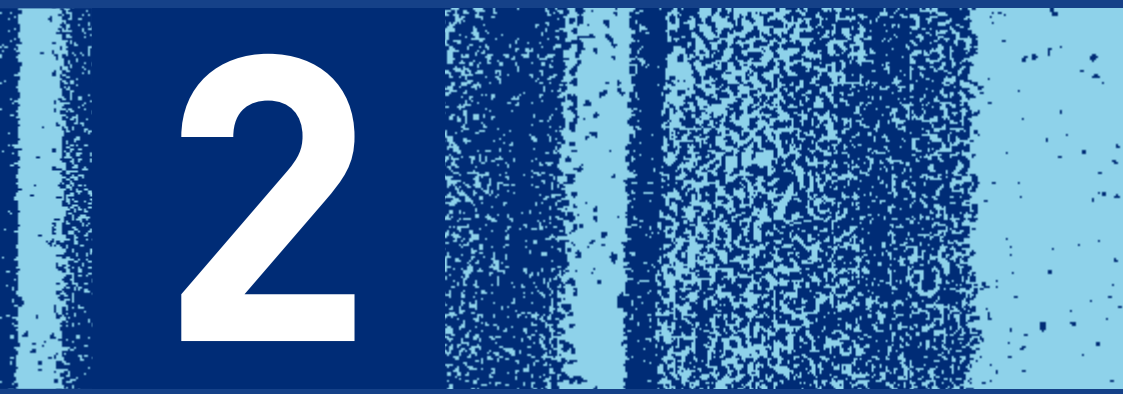


[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in June 2016. Android-PUP/SmsPay was the most distributed malware with 84,728 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	84,728
2	Android-PUP/Zdpay	20,401
3	Android-Trojan/Moavt	19,027
4	Android-PUP/Noico	18,709
5	Android-PUP/Skymobi	18,456
6	Android-PUP/SmsReg	17,203
7	Android-Trojan/Hidap	14,132
8	Android-PUP/Shedun	14,043
9	Android-Trojan/AutoSMS	11,429
10	Android-Trojan/Agent	10,030



2

SECURITY ISSUE

Cross-platform Adware Appears

SECURITY ISSUE

Cross-platform Adware Appears

With the increasing diversification of operating systems including mobile OS, iOS and Android, as well as ARM architecture-based processors, "cross-platform" malware, which can skip across different OS unbound by platform restrictions, continue to increase. Recently, even an adware has appeared as a type of cross-platform malware.

Pirrit, an adware discovered by the security vendor Cybereason, was developed using a cross-platform framework. Since Pirrit adware was first discovered in 2014, it has targeted Windows platform and continued to surface. The adware is installed on the back of a variety of programs, and modifies the proxy settings of a system's Web browser and displays an advertisement popup while the user is surfing the Web.

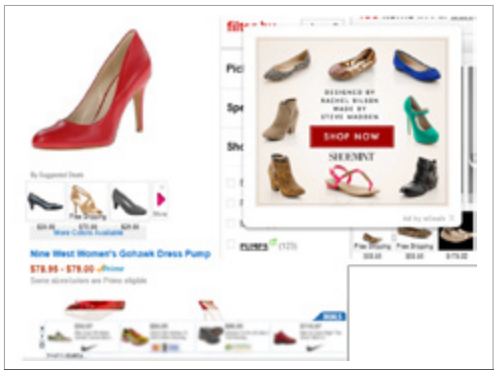


Figure 2-1 | Popup of Pirrit Adware for Windows OS (*Source: Microsoft.com)

The recently-discovered Pirrit for OS X on the Mac is also presumed to have been disseminated while hidden inside a variety of utility programs, and was created using Qt, a cross-platform development framework, as shown in Figure 2-2.

Figure 2-2 | Qt 4 cross-platform development framework

Parsing through the adware's string indicates that it includes a Windows registry key despite being an adware that runs on OS X, as shown in Figure 2-3.

Figure 2-3 | Windows registry key values embedded in Pirrit

While the Mac version Pirrit, like its Windows version, attempts to modify proxy settings, however, it uses a different method including running the http proxy server as port 9882 to route the http traffic on the system.

Figure 2-4 | Proxy server processes

As more people has used a diverse array of devices and operating systems, the scope of security issues has also been expanding. Mac OS is still widely regarded as more secure than Windows; a closer examination of malware for Mac systems being discovered in recent days, however, show that these malware, while less common, still have the same functions and methods. The increasing use of open source and cross-platform development frameworks has led to a rise in the number of malware targeting non-Windows systems. Users who use Mac OS or other operating systems should remain vigilant when installing new programs or running files attached to suspicious or spammed email.

The relevant aliases identified by V3 products, AhnLab's anti-virus program, are as below:

<Aliases identified by V3 products>
OSX64-Adware/DLNow.141732 (2016.06.03.00)
OSX64-Adware/Pirrit.414196 (2016.06.03.00)

3

IN-DEPTH ANALYSIS

Ransomware Using "Malvertising" Plague Users

IN-DEPTH ANALYSIS

Ransomware Using "Malvertising" Plague Users

We are more than halfway through 2016, attacks from ransomware, malware that hold a user's file hostage and demands payment for their release, show no signs of letting up their relentless attack. Ransomware attacks frequently take place via spammed emails and website that are compromised by "malvertising". In spam mail, the attacker sends scripts as file attachments to a large number of random recipients; when a user unwittingly runs the attachment, the system is infected with ransomware. Malvertising, on the other hand, disseminated ransomware via advertisements inserted into Web pages.

Malvertising, a portmanteau of the words "malware" and "advertising", is much more widely destructive than attacks via spammed emails. In Website advertisement, one ad server beams ads to a number of Web pages, which are exposed to a large number of users in a short span of time. This mechanism can infect a user's system with ransomware even no suspicious file has ever been downloaded or executed. With malvertising technique becoming worrisomely more frequent, a closer examination is warranted.

An ad server is tasked with transmitting pre-prepared ad content onto the advertising space on a Web site. The attacker sends a malware exploit kit and a normal ad panel to an ad server. When a user visits the Web page containing the ad, the server sends the normal ad with its hidden exploit kit to the Web page. When this page is accessed with the user's Web browser, a drive-by-download method that takes advantage of security vulnerability is used to infect the user's system.

Figure 3-1 shows network information collected from a recent malvertising

attack. The site, "www.livead*********.com", is an ad server that displays advertisements on Web pages.

Figure 3-1 | Malvertising network information

The ad server receives the request for an advertisement page from the user's Web browser, and duly sends the page. The ad page contains both a Web site, "tom****.com", and "108.**.***.63" ,the origin point of the malware.

Table 3-1 | Received advertisement information

[www.livead*********.com/a/display.php]

```
<html>
<head>
<title></title>
   <link rel="dns-prefetch"
href="http:\/\/tom****.com\/*********************
*****************trackurl.php
... ...
```

The ad page is designed to access "tom-****.com", as shown in Table 3-1.

Table 3-2 | tom****.com page information

[tom****.com.../trackurl.php]

```
<html>
<head>
<script type="text/javascript"
src="http://108.**.***.63/"></script>
<meta http-equiv="refresh" content="8;http://www.
tom***.com/******************">
</head>
</html>
```

The linked "tom****.com" site is also designed to connect to "108.**.***.63", which is the originator of the malware.

Table 3-3 | vnunfse.**********.top page information

[vnunfse.**********.top]

```
<html>
<body>
... ...
   <param name="bgcolor" value="#ffffff"/>
   <param value="always"
name="allowScriptAccess"/>
   <embed src="/****************/likewise-
**************-granny-pale-cottage.swf"
... ... width="533" allowScriptAccess="sameDomain"
quality="high" height="120" loop="false"/>
</object>
</body>
</html>
```

A flash file runs in the final page where the user lands, and the ransomware is executed via drive-by-download. Then ransomware encrypts important files on the victim's system, and then displays a "pay-up" warning dialogue as shown in Figure 3-2.

Figure 3-1 | Malvertising network information

Ransomware attacks are becoming increasingly prolific. To prevent damages from ransomware infections, anti-virus program should be installed and kept AV engine always up to date. Security updates for the operating system, browser and major applications should be applied. Also, users should avoid running files attached to suspicious emails and visiting Web sites with questionable security. Work-related files, confidential documents, various images and other important files should be backed up regularly, with secondary off-site backup.

The relevant alias identified by V3 products, AhnLab's anti-virus program, is as below:

<Alias identified by V3 products>

Win-Trojan/CryptXXX.Gen

AhnLab

ASEC REPORT

VOL.78
June, 2016

Contributors	**ASEC Researchers**	Publisher	**AhnLab, Inc.**
Editor	**Content Creatives Team**	Website	**www.ahnlab.com**
Design	**Design Team**	Email	**global.info@ahnlab.com**