Security Trend

ASEC REPORT

VOL.63

March, 2015

AhnLab

ASEC REPORT

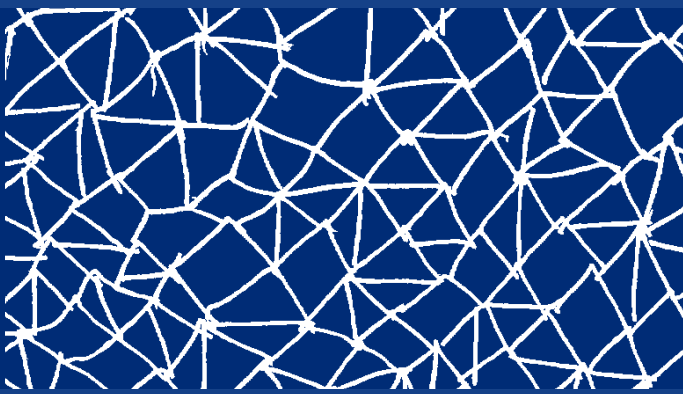
VOL.63 March, 2015

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 MARCH 2015

Table of Contents

1

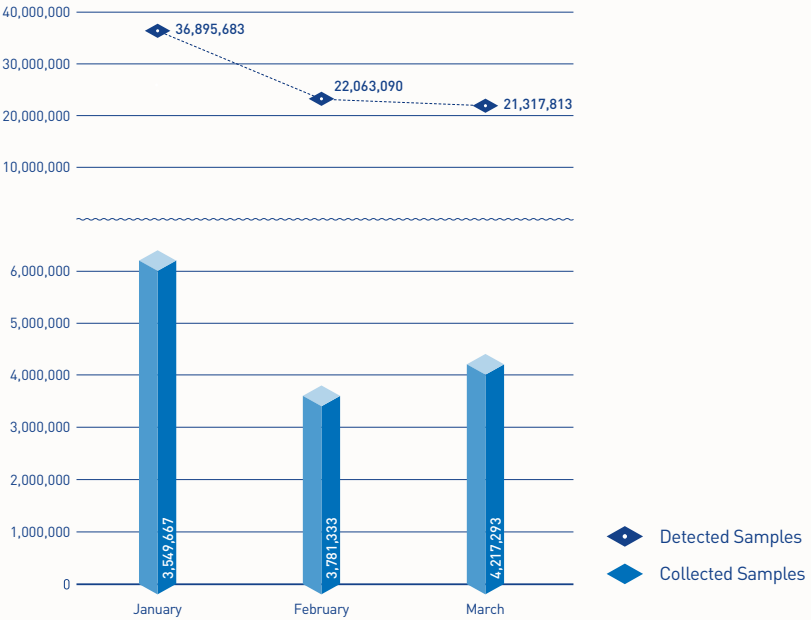


SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

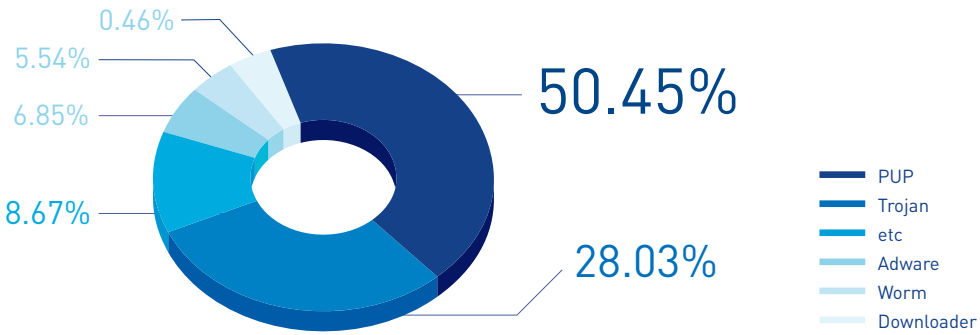
According to the ASEC (AhnLab Security Emergency Response Center), 21,317,813 malware were detected in March 2015. The number of detected malware decreased by 745,227 from 22,063,090 detected in the previous month as shown in Figure 1-1. A total of 4,217,293 malware samples were collected in March.



[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 March 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 50.45% of the total. It was followed by Trojan (28.03%) and Adware (6.85%).



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

Table 1-1 shows the Top 10 malware threats in March categorized by alias. PUP/Win32.MyWebSearch was the most frequently detected malware (2,086,933), followed by PUP/Win32. MicroLab (1,632,730).

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

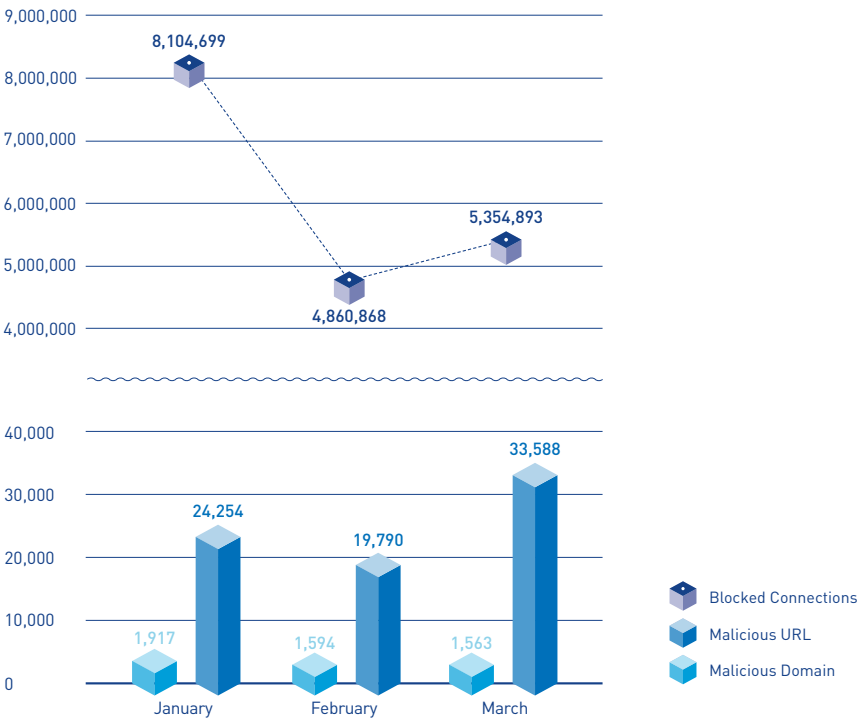
Rank	Alias from AhnLab	No. of detections
1	PUP/Win32.MyWebSearch	2,086,933
2	PUP/Win32.MicroLab	1,632,730
3	PUP/Win32.BrowseFox	1,423,302
4	PUP/Win32.Helper	896,322
5	PUP/Win32.Enumerate	772,126
6	PUP/Win32.SubShop	541,662
7	PUP/Win32.IntClient	516,121
8	PUP/Win32.Generic	514,346
9	PUP/Win32.Gen	405,807
10	PUP/Win32.CloverPlus	398,999

SECURITY STATISTICS

02

Web Security Statistics

In March 2015, a total of 1563 domains and 3,3588 URLs were comprised and used to distribute malware. In addition, 5,354,893 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.

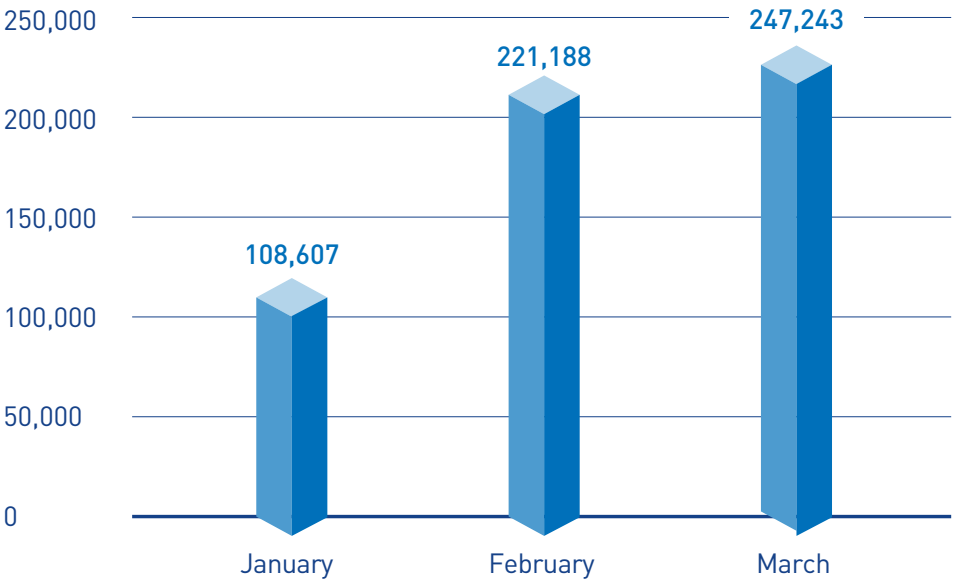


[Figure 1-3] Blocked Malicious Domains/URLs in March 2015

SECURITY STATISTICS

03 Mobile Malware Statistics

247,243 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 March 2015. Android-PUP/SmsReg was the most distributed malware with 152,962 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SMSReg	152,962
2	Android-PUP/Noico	14,083
3	Android-Trojan/FakeInst	12,319
4	Android-PUP/Dowgin	9,480
5	Android-Trojan/AutoSMS	6,176
6	Android-PUP/Airpush	4,041
7	Android-Trojan/Opfake	3,723
8	Android-PUP/Wapx	2,738
9	Android-Trojan/SMSAgent	2,641
10	Android-Trojan/SmsSend	2,152

2

SECURITY ISSUE

More Powerful Pharming Attacks

SECURITY ISSUE

More Powerful Pharming Attacks

1. LSP Modification Pharming

An older method of attack used by malware in online game hacks and pharming attacks has recently been rediscovered. The newest incarnation involves a method using an LSP (layered service provider), and a method using normal files. Let's examine both.

Before delving into the actual malware, a review of the structure of an LSP can be illustrated as follows in [Figure 2-1]

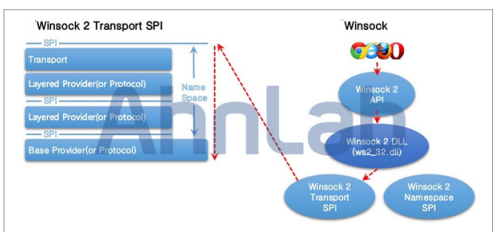


Figure 2-1 | Winsock 2 & Winsock 2 Transport SPI structures

Winsock (Windows Socket API) is an interface that processes the input and output requests of Internet applications in the Windows OS environment. Winsock intercepts commands from applications such as Web browsers, which is passed through "Winsock 2 DLL" to eventually communicate with the "base provider".

Since all data can pass unfiltered through the LSP as part of this communication process, all inbound and outbound data can be monitored. Unauthorized deletion of an LSP prevents the network from functioning properly; in addition, since the LSP is written into the register, detecting the modification of an LSP is difficult.

The malware that was recently discovered uses the traditional "LSP modification" and "VPN tunneling" methods of attack. A malware infection creates the following files, as shown in [Table 2-1].

Table 2-1 | Paths where files are created

[Created Files]
C:₩WINDOWs₩system32₩v2BSXerv.dll
C:₩WINDOWs₩system32₩twlsp.dll

The files that are thus created are written into the registry as in [Table 2-2], and run automatically at system startup.

Table 2-2 | Writing to registry

[Registry Paths]
HKLM₩SYSTEM₩ControlSet001₩Services₩BSXerv₩DisplayName
→"BS Server"

HKLM₩SYSTEM₩ControlSet001₩Services₩BSXerv₩ImagePath
→"%SystemRoot%₩system32₩svchost -k BSXerv"

HKLM₩SYSTEM₩ControlSet001₩Services₩BSXerv₩Parameters₩ServiceDll
→"C:₩WINDOWS₩system32₩v2BSXerv.dll"

Next, the system's LSP is modified. The malware erases all LSP protocol information stored in the system and adds the file "twlsp.dll". The LSP protocol information that has been previously stored is then restored.

Table 2-3 | Modified LSP Path

[Modified LSP Path]
HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\[number]\PackedCatalogItem
→ 43 3A 5C 57 49 4E 44 4F 57 53 5c 73 79 73 74 65 6d 33 32 5c 74 77 6c 73 70 2e ...(etc.)

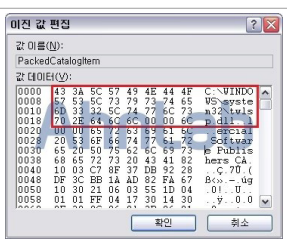


Figure 2-2 | Added 'twlsp.dll' file

The malware then deleted itself to prevent the user from detecting the infection. Next, the infected system receives VPN information via "v2BSXerv.dll", executed through svchost.exe, and attempts to make a connection.

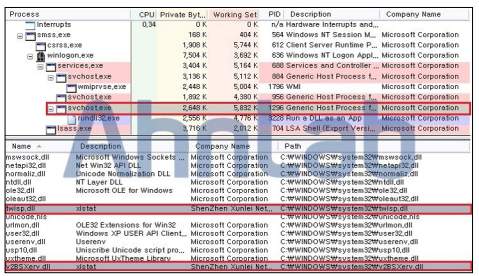


Figure 2-3 | 'v2BSXerv.dll' being executed

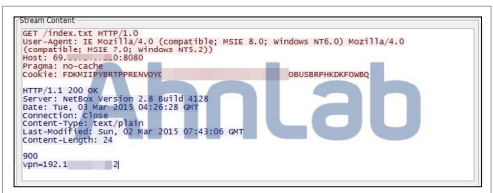


Figure 2-4 | Receiving VPN information

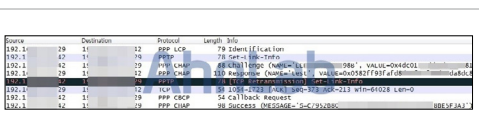


Figure 2-5 | Attempting to connect to a VPN

Once connected to a VPN, the malware monitors the infected system for an attempt to connect to the Web pages of major portals or financial institutions. When the user tries to connect to

the website, the malware hijacks the connection and directs the user to a pharming site.

When the user access the pharming site via the financial institution's image, the malware acquires the user's personal financial information. A PC with deficient security protection can be infected with this type of malware by merely visiting the website. To avoid being infected, the user must keep applications carefully updated and only visit sites that are verified to be safe.

Figure 2-6 | Malware distribution process

2. Pharming Attacks Using Normal (UTIL) Files

Several websites in Korea were recently found to have been used over a weekend to distribute pharming malware. The majority of the sites were modified to ultimately download the same malware.

The actual method of distribution is similar to the method for malware distribution using "Caihong & God Mode". The attacker injects an inline frame into a vulnerable website, and after passing through other sites the system is lured into downloading a pharming malware.

The injected scripts are obfuscated to make analysis difficult. Ordinary users cannot observe the actual script being run and thus is unable to realize that a malware infection has occurred. The pharming malware that was discovered recently used ordinary utility files as part of the execution process.

Of course, this is not the first instance of normal files being used to execute malware. In 2014, the files of a well-known program in Korea was used to run malware, and the latest discovery uses "Volumouse Utility" a utility for adjusting

speaker volume with the mouse, to run the malware.

Figure 2-7 | DLL Load

This exploit uses a design flaw where the DLL is not verified when it is loaded by a normal file. Volumouse.exe loads and runs vlmshlp.dll, but does not perform a verification check of the file during the loading process. Thus a file that is not part of the normal operational design will still be run as long as it has the same name as the legitimate DLL to be loaded.

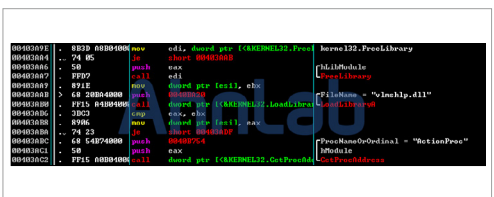


Figure 2-8 | Loading the malicious vlmshlp.dll

The malicious vlmshlp.dll that is loaded as shown in [Figure 2-9] executes svchost.exe, and transforms it into a malicious process through memory corruption.

Figure 2-9 | Executing the corrupt svchost.exe

Since only the data in the memory area is corrupted, the file itself is normal but the actual process is altered by the corrupt vlmshlp.dll. It is difficult for the ordinary user to determine whether the vlmshlp.dll is legitimate or malcious.

Ultimately, the corrupt svcshost.exe tricks the user into accessing pharming sites by leaking the public key certificate stored in the system, altering the DNS, and extracting the MAC address to steal the user's financial information.

These methods that invade legitimate websites to distribute malware exposes every user to access the site as targets for attack. These attacks exploit vulnerabilities in particular application programs and operating systems to distribute malware without alerting the user. Since the infection is difficult to detect, the user's system can be made defenseless to the malware unless security updates are performed

or vaccines used. To prepare for such attacks, it is advised that security updates and vaccines are always kept up to date with the latest release versions.

The Ahnlab range of V3 products detects the following malware aliases:

<Aliases Detected by V3 Products>

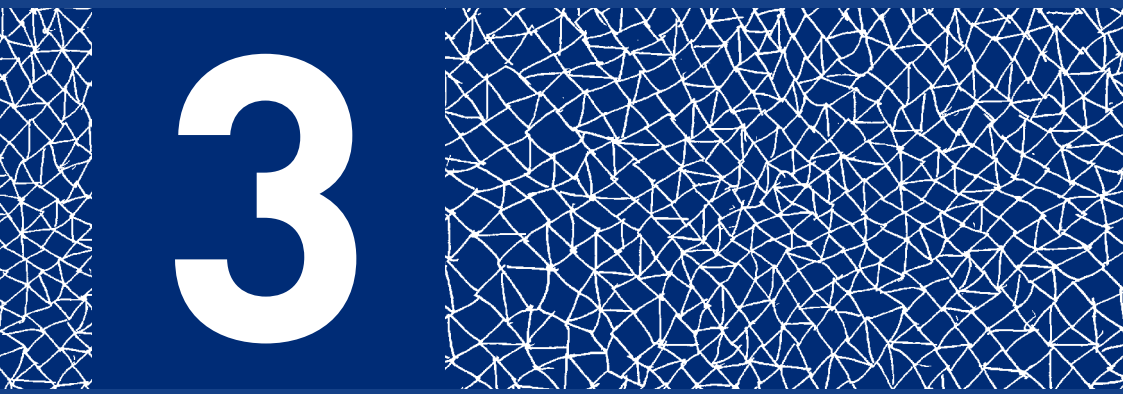
Trojan/Win32.Kryptik (2015.03.04.00)

Trojan/Win32.Injector(2015.03.09.03)

Trojan/Win32.Banki(2015.03.10.04)

JS/Redirect(2015.03.10.02)

JS/Exploitkit(2015.03.09.02)



3

IN-DEPTH ANALYSIS

Symptoms and prevention of AUTOCAD malware infection

SECURITY ISSUE

Symptoms and prevention of AUTOCAD malware infection

AUTOCAD, a design program, has less users than Photoshop or Office suite programs, making it more difficult for the user to be aware of an infection. Companies that use AUTOCAD often do not immediately realize that a malware infection has occurred. The malware is program-specific, in this case AUTOCAD, as the "LISP" (list processor) file that is often detected as malware does not affect other programs but is automatically loaded when a drawing file (*.dwg) is opened.

Since the malware's purpose is to inhibit certain command executions of drawing files or to distribute LISP files, it is difficult for the ordinary PC user to detect the infection. Thus the malware is frequently not discovered until a period of time has passed and multiple AUTOCAD users have become infected. The following examines the symptoms of such an infection and how it can be prevented.

There are many file names that have been associated with AUTOCAD malware, but the most common are as show in [Table 3-1].

Table 3-1 | Common file names used by AUTOCAD malware

acad.lsp, acaddoc.lsp, acadapp.lsp, acadapq.lsp, acadiso.lsp, acad.dvb acad.fas, acaddoc.fas, acad.vlx, acadiso.lsp, acad.mnl

Symptoms that occur when drawing files contained in a folder infected with malware are as outlined in [Table 3-2].

Table 3-2 | Major symptoms of AUTOCAD malware infection

1	LISP files created in all drawing folder paths.
2	Some command prompts rendered unusable (EXLODE, XREF, XBIND, etc.)
3	Unrecognizable error string and pop-ups
4	Changes to system variables (ACADLSPASDOC, FILLMODE, etc.)
5	Load error messages (acaddoc, acadapp, acadapq)
6	"Initializing VBA system...Execution error" error message prompted (automation error occurs while loading VBA)
7	Error: stringp nil
8	Program lockup or delay occurs when loading a drawing file

When an infection by an AUTOCAD malware occurs, LISP files are created in the folder paths where drawings are stored as indicated in [Table 3-2]. Let's examine some of the symptoms listed above.

1. acad.lsp Sample

A main symptom of the malware "acad.lsp" which was recently reported to AhnLab is as follows. First, this particular malware copies itself to <AutoCAD Folder\Support\acadapp.lsp>, then modifies the files in <AutoCAD Folder\Support\acad.lsp>as show in in [Figure 3-1]

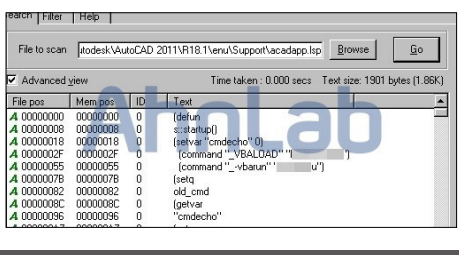


Figure 3-1 | Part of the contents of acadapp.lsp

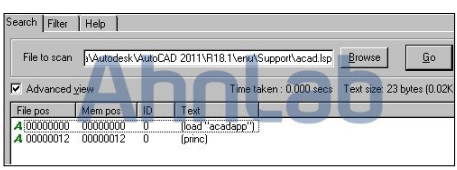


Figure 3-2 | Contents of acad.lsp

Next, the message "error: bad argument type: string nil" is displayed when a drawing file is loaded, as noted in item seven on [Table 3-2].

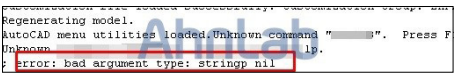


Figure 3-3 | stringp nil error

Or, the message "Initializing VBA System...Execution error" will be displayed, as noted in item six on [Table 3-2].

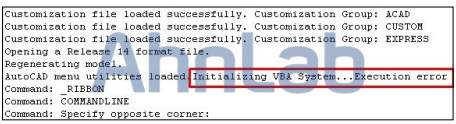


Figure 3-4 | Initializing VBA System...Execution error

Even if the acad.lsp file in [AutoCAD Folders\Support\acadapp.lsp] or other folders is deleted, a "Load failed" error message ([Table 2-2]) may be displayed unless the file in [AutoCAD Folders\Support\acad.lsp] is not modified.

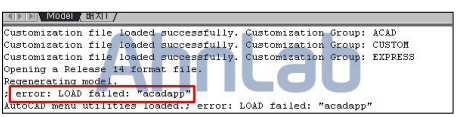


Figure 3-5 | Load failed error

2. acad.fas Sample

Another malware, "acad.fas", shows the following symptoms. As indicated in item three of [Table 3-2], the 'ACADLSPASDOC' variable value is changed from 0 to 1.

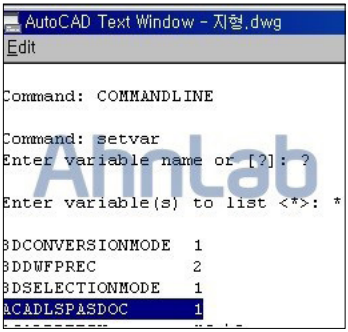


Figure 3-6 | System variable altered

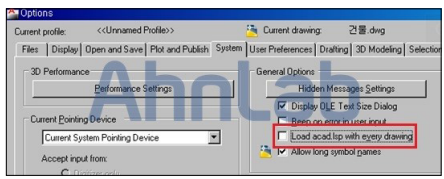
3. Preventing an AUTOCAD malware infection

An AUTOCAD malware infection as shown above can cause considerable inconvenience to the user by preventing the normal loading of drawing files or the operation of certain commands. Methods for preventing AUTOCAD malware infections are as follows;

1. Check the contents of a file before running a drawing file if there is a LISP file that has not been created by the user in the folder.
(LISP files automatically loaded at AutoCAD starup :acad.lsp, acad.fas, acaddoc.lspacad.dvb, acaddoc.vlx, acaddoc.fasetc.)

2. Create empty LISP files as "read-only" files and name them with the file names frequently used by malware.

3. Change AUTOCAD options. Uncheck the option [Load acad.lsp with every drawing].



4. Set the value of the system variable ACADLSPASDOC as 0.
- Can be verified by Command :setvar -> ? -> *

5. Use *.mnl files or *.lsp files being run as read-only.

6. Avoid the use of shared folders, since AUTOCAD malware, like a virus, can replicate itself.

Numerous companies, in fact, often set their drawing folders as shared folders to facilitate their business process. This may result in malware infecting every user, and simply not using a shared

folder can prevent the additional spread of malware.
Any organization that uses AUTOCAD should disable shared folders, and it would be prudent to refrain from running unverified VBA scripts when running AUTOCAD.

The Ahnlab range of V3 products detects the following malware alias:

<Alias Detected by V3 Products>
ALS/Bursted

AhnLab

ASEC REPORT

VOL.63
March, 2015

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