방송통신위원회
KOREA COMMUNICATIONS COMMISSION

January 12, 2012 (Thursday)

Press release

To be reported at or after 11:00, January 12, 2012 (Thursday).

Inquiry: in-Bae Hong, Internet Pilicy Division, Network Policy Bureau (☎750-2730)
Hyeon-Seon Park, Internet Policy Division (☎750-2723) phsunny@kcc.go.kr

According to the 2011 probe into malicious code removal programs, removal performance has improved overall but products have been increasingly issuing false alerts.

- Users need to be cautious about poor vaccines and products issuing false alerts -

During the second half of 2011, the Korea Communications Commission (Chairman See-Joong Choi) in conjunction with the Korea Internet Security Agency (President Simon Suh) investigated 202 malicious code removal programs made and sold in Korea, and found that the malicious code removal performance has improved compared to 2010, but products are increasingly issuing false alerts and faulty vaccines are still being made and distributed.

■ **Outline of the investigation**

① Period: September 1, 2011 ~ December 31, 2011

② Targets: 202 programs from 77 companies (subscription-based or purchase-only 181, free 21)

③ Investigation items : 39 items including malicious code detection and removal performance, provisions of the user agreement, user consent to installation, updates, and real-time detection capability were investigated <See Attachment 1>

As for malicious code detection and removal, the number of programs that detected and removed more than 2/3rd (2,000) of 3,000 new malicious code samples about doubled as compared to 2010 (17.5% → 31.2%), and the number of vaccine programs with real-time monitoring effectiveness also increased (16% → 26.7%). However, the number of programs with automatic updates decreased (64.6% → 45%), and the number of products issuing false-alert that mistake a normal file as malicious and cause damage to users also greatly increased (27.7% → 52%). So users need to pay a great deal of attention when choosing a product. (See <Attachment 5> 10 rules to follow when using vaccine programs.)

※ The malicious code samples used in the test include samples actually used in intrusion incidents, samples discovered in two or more foreign locations, and new malicious codes detected by 3 or more vaccine engines.

The Korea Communications Commission is planning to pick the top 12 products out of 63 that detected and removed more than 2/3rd of the 3,000 samples in this test and meet other essential requirements such as user agreement notification and consent for installation, and post the 12 products on the KISA Boho Nara website (http://www.boho.or.kr/) so that users can use this information when selecting products.

The Korea Communications Commission notified the test results to each of the manufacturers of products that had problems like false alerts and inadequate performance, and recommended them to take corrective measures. KCC is also planning to cooperate with relevant agencies (the National Police Agency, the Korea Consumer Agency, etc.) to minimize damages to users.

Furthermore, KISA will post its *Casebook of Damage Caused by*

Faulty Vaccines based on customers' complaints about damages related to malicious code removal programs on the Boho Nara website to prevent similar damages and help users effectively cope with them.

The Korea Communications Commission said, "The *Vaccine Program Users Guide* distributed last September and the *Casebook of Damage Caused by Faulty Vaccines* will help users be better informed about the safer vaccines available and how to use them more effectively. Also, the Malicious Program Expansion Prevention Bill currently being reviewed by the National Assembly should be passed soon so that a more fundamental solution to the problem will exist."

Attachment: 1. Report of the 2011 malicious code removal program investigation.

2. List of items (39) checked in the malicious code removal program investigation

3. List of programs (12) with high malicious code removal rates

4. Comparison of the results of the malicious code removal program investigation.

5. 10 rules for choosing and using vaccine programs.

〈Attachment 1〉

Results of the 2011 investigation of malicious code removal programs

□ Background

o To prevent faulty vaccine programs from causing damage to users, improve the performance of vaccine programs available in the market, drive out under-performing vaccines, and provide users with information on excellent vaccines, KCC has conducted a thorough investigation into the vaccines available on the open market.

※ This investigation began in 2006 after civil complaints about the flood of false and faulty spyware removal programs had increased dramatically. The National Assembly pointed this out during a parliamentary inspection, so the investigation was extended in 2009 to include malicious code removal programs.

〈Spyware〉

This is a word formed by combining 'spy' with 'software.' Originally such programs were intended to steal personal information, but as the Internet environment has evolved, it now includes programs that are covertly installed on users' PCs to initiate malicious acts such as arbitrarily changing the Internet start page, display an advertising page, or leak personal information.

□ Outline of the study

o Targets : **202 vaccine programs from 77 companies available in the market as of August 2011** (181 subscription-based or purchase-only programs, and 21 free programs)

※ The number of companies (93→77) and products (206→202) decreased as compared to 2010.

- However, programs offering privacy protection solutions or PC performance optimization services only were excluded.

o Investigation items : 39 items including malicious code removal rate

(3,000 samples), real-time automatic update, and terms of the user agreement.

※ The number of malicious code samples was increased in 2011 from 2,000 in 2010 to 3,000 in 2011.

o Characteristics : in-depth investigation, e.g. comparison of user agreements on the website/during program installation/in relation to automatic payment, and use of a "clean/dirty" system to check for false alerts, etc.

※ Clean system : virtual machine testing environment not infected with any malicious code
Dirty system : virtual machine testing environment infected with a number of malicious codes

□ Results of the investigation

o **(Diagnosis and removal performance)** Malicious code detection and removal rates were investigated and the results showed that the number of under-performing products significantly decreased as compared to 2010, and their overall performance improved.

- 63 programs (31%) detected and removed more than 2,000 (2/3) of 3,000 new malicious code samples, up from 36 (18%) in 2010.

※ It is believed that the overall removal rate improved because new vaccine programs adopted foreign engines with excellent removal performance.

- **118 (58%) products out of 202 were under-performers** (they removed less than 1,000 of the 3,000 malicious code samples)

※ In particular, 82 products (41%) removed less than 10 out of 3,000 malicious code samples.

※ The performance of 15 products out of 202 could not be verified, so they were excluded from the test.

〈 Under-performing products or products whose performance could not be verified 〉

Classification	1sthalfof2007	2ndhalfof2007	1sthalfof2008	2ndhalfof2008	1sthalfof2009	2ndhalfof2009	2010	2011
Removed less than 10	78 (66%)	81 (68%)	80 (66%)	86 (67%)	86 (64%)	108 (68%)	135 (66%)	82 (41%)
Performance could not be verified	11 (9%)	7 (6%)	11 (9%)	16 (13%)	18 (13%)	14 (9%)	14 (7%)	15 (7%)
Total number of products	118	119	122	128	134	160	206	202

- However, the number of false-alert products tested in the **clean system rose from 57 (27.7%) in 2010 to 105 (52.0%).**

※ 105 false-alert products included 50 new products released in 2011 and 55 existing products (22 products were not improved, and 33 products actually became worse).

※ Criteria of false alerts: ① In the cleaner test, parts of the registry and some files (not actual malicious code) are detected as malicious, and ② as some registry entries and simple files are targeted for removal to optimize PC performance, users are likely to be confused.

※ Users need to exercise caution as they are enticed to make an unnecessary payment under the pretext of registry and system optimization.

- The number of products with the real-time detection increased from 33 (16.0%) in 2010 to 54 (26.7%).

o **(Makers by product)** Most of the companies selling many similar products are makers of under-performing products that are likely to cause damage to users.

- 33 out of 77 companies are making and selling at least two products each, and the number of products released by them is 156, accounting for 77.2% of the total.

- In particular, only 54 products out of 156 from 33 companies are ranked high in terms of removal rate (removal of more than 2,000 malicious code samples).

- Six companies are distributing several products based on whether they are free, purchased only or subscribed to, and whether they are downloaded or installed from a CD. Generally speaking, there is not much difference among the products of 27 companies.

o **(Customer support)** A user agreement, privacy policy, and contact email address and/or phone number for responding to customer queries or complaints were available for most products, but;

- Only 17.8% of the companies replied to email enquiries, while 57.8% of them answered phones.

o **(Program installation)** Cases of no user agreement during installation directly related to users' complaints, no consent to installation, and installation of additional programs have continued to decrease after 2006.

< Key issues related to program installation >

Item	1st halfof 2006	1st halfof 2007	2nd halfof 2007	1st halfof 2008	2nd halfof 2008	1st halfof 2009	2nd halfof 2009	2010	2011
No user agreement during installation	38.7%	38.1%	41.2%	31.1%	21.1%	9.7%	12.5%	3.4%	2.0%
No consent to installation	38.7%	40.7%	34.5%	20.5%	12.5%	11.2%	12.5%	1.9%	1.5%
Installation of additional programs	21.5%	16.9%	11.8%	8.2%	4.7%	4.5%	5.6%	1.0%	1.0%
Installation of additional programs without user consent	8.6%	5.9%	1.7%	0.8%	0.0%	0.0%	0.0%	0.0%	0.5%

- According to the 2011 investigation, only 7 programs were installed without any user agreement or consent, and 2 products installed additional programs besides the main program.

o **(Complaints)** The number of civil complaints received by the 1372 Consumer Consultation Center and the Korea Consumer Agency vaccine program dropped considerably as compared to 2010.

< Complaints related to vaccine programs >

Classification	1372 and KCA		118 Center	
	Jan 2010~Nov 2010 (11 months)	Dec 2010~'Oct 2011 (11 months)	Jan 2010~Dec 2010 (12 months)	'11.1.~'11.12. (12 months)
Number of complaints related to vaccines	612	248	85	45
Number of programs that can be confirmed (including redundancy)	277	129	100	58
Number of programs to be investigated (including redundancy)	268	98	94	53

o **(Follow-up measures)** As for the 130 vaccine programs that were under-performing, issued false alerts, and/or were installed without users' consent, KCC **notified the results of the investigation to the related companies**, and requested them to take corrective measures.

- 16 out of 56 target companies replied.

〈 Replies 〉

Classification	Targets	Official replies	Completed improvements
False alerts	105 programs of 47 companies	39 programs of 16 companies	11 programs of 5 companies
Under-performance	83 programs of 39 companies	12 programs of 9 companies	1 program of 1 company
Installation without consent	2 programs of 2 companies	0 programs of 0 companies	0 programs of 0 companies
Total	130 programs of 56 companies	40 programs of 16 companies	11 programs of 5 companies

□ Selection of excellent programs

o As a result of the investigation to help users correctly select and utilize vaccine programs and prevent faulty vaccines from causing damage to users, the 12 best programs were selected and announced.

- The 12 best programs that met or exceeded the excellent-performance criteria were selected for special attention.

〈 Criteria for selecting excellent programs 〉

Criteria	Details
Removal of more than 2/3	Detected and removed more than 2,000 out of 3,000 new malicious code samples ※ The same criteria as in 2010 (more than 1,333 of 2,000 samples)
Compliance with essential requirements	Programs that meet essential requirements such as installation with the consent of the user, clear user agreement, registry/file scan, and minimal number of false alerts
Real-time detection capability	Capability to detect threats in real time (i.e. ability to respond to hidden malicious codes such as RootKit)
Reliability	Programs of companies consumers cannot trust for the following reasons are excluded. - Companies with a program distribution problem (i.e. companies distributing programs subject to follow-up measures) - Companies distributing programs with conspicuously poor removal performance (i.e. companies receiving an above average number of related complaints)
Service continuity	Products that were serviced during the investigation but were not after the results were announced, were excluded.

o 12 excellent programs from 11 companies

Program name	**Company name**	**Charged/free**
Daum Toolbar	Daum Communication	free
NoAd2+	MirageWorks	charged
V3 365 Clinic, V3 Lite (2)	Ahn Lab	charged/free
Virus Chaser 8.0	SGA	free
Alyak 2.0	ESTSoft	free
nProtect AVS 3.0	Inca Internet	charged
ViRobot Internet Security 2011	Hauri	charged
My Family Doctor	KT	free service by ISP
U+ Internet PC Ansimmi	LG U+	charged service by ISP
Naver vaccine	NHN	free
B Internet Clean	SK Broadband	free service by ISP

※ **Company names are** in alphabetical order (Korean and English), and charged/free classification is for personal users.

□ Implications

o In general the performance of vaccine programs available in the market has **improved** year after year, and complaints have been decreasing gradually. **Users seem to be better aware of faulty vaccines**, but,

- Still **many un-reputable companies** seeking only quick monetary gains **are releasing ineffective and potentially damaging vaccine programs** into the market.

- The investigation revealed that supplementary measures were requested to address under-performance, false alerts, and installation of vaccine programs without consent, but **few have been improved**.

o It is difficult to find facts about and respond to faulty vaccines that are distributed through channels other than websites such as affiliated programs, and,

- KCC invests a lot of time and manpower each year to conduct the investigation, but it is limited in its ability to perfectly prevent damages due to faulty vaccines.

※ Activities to enhance awareness such as notification of the results of the investigation, recommendation of improvements, media coverage, and distribution of guidebooks and casebooks are limited in their ability to solve the problem.

※ There should be legal means developed for the Korea Communications Commission to directly regulate faulty vaccines (Currently, faulty vaccines are indirectly regulated by the National Police Agency and the Korea Consumer Agency.)

〈Attachment 2〉

Malicious code removal program investigation items (39)

○ No.	Large category	Small category	Inspection item	Description
1	Website	Notification	User agreement	whether the website has a user agreement (O/X)
2			Privacy policy	privacy policy is provided through Check Privacy (O) privacy policy is merely posted on the website (△) privacy policy is not posted on the website (X)
3		Response to complaints	Phone number	whether phone number is provided on the website for users to call. on the homepage (O), on a page other than the homepage, (△), not provided (X)
4			Answering phones	whether phone calls are answered when users call the company (O/X)
5			email	whether the website provides a contact email for users (O/X) on the homepage (O), on a page other than the homepage, (△), not provided (X)
6			email reply	whether email inquiries are answered when website users sent email (O/X)
7			Bulletin board	whether the website has a BBS or FAQ for inquiries (O/X)
8		Introduction	Quality certification	whether the program has been officially certified (O/X)
9			Instructions	whether information like how to use and install the program is available on the website (O/X)
10			Supported OS	whether the website explains the supported OS (O/X)
11		e-commerce	Company name	company name related to Internet business available on the website (O/X)
12			Name of representative	name of representative related to Internet business available on the website (O/X)
13			Address	address of the Internet business available on the website O/X)
14			Business license number	business license number of the Internet business available on the website (O/X)
15	Management	Distribution	Distribution method	program distribution type (EXE/ActiveX/EXE&ActiveX)
16			Code signing	application of code signing to verify who posted the program (O/X)
17		Installation	Installation with consent	whether the program's own confirmation window is displayed when the program is installed (O/X) (If IE's own function confirms installation of ActiveX, it is regarded as non-consent)
18			User agreement during installation	whether the user agreement is clearly specified during installation O/X)
19			Possible to know the installation path	whether it is possible to know the path when the program is installed (O/X)
20			Installation of additional programs	whether additional programs are installed when the program is installed (O/X)
21		Advertising	Exposure to advertising windows	whether an advertising window is displayed when the program runs (O/X)
22		Deletion	Program removal function	whether an uninstall option is provided in the menu, control panel and/or website (O/X)
23			Support for complete program removal	the program is completely deleted (O) if information about the program remains in the menu, wallpaper and control panel, or the execute file remains in a folder (X)
24		Payment	Pricing policy	weekly, daily and monthly subscription pricing policy
25			Payment method	payment methods available (i.e via phones, ARS and mobile phones, etc.)
26			Automatic extension of use	whether there is automatic renewal (O/X)
27	Function	Updates	Support of automatic update	whether automatic updates are included (O/X)
28			Pattern updates and log	users can check updates after pattern update (O) pattern update is done, but users cannot check it (△) pattern update is not done after a certain amount of time (X)
29		Diagnosis	Support of schedule check	whether schedule check function is provided (O/X)
30			Able to select diagnosis areas	whether selective diagnosis is provided for multiple drives (i.e. USB drives, etc.) (O/X)
31			Registry/file scan	whether malicious codes are scanned by monitoring activities related to registry/file (O/X)
32			Provision of diagnosis details	diagnosed malicious code and registry location information are provided (O) only part of the paths for diagnosed malicious code files and registries is provided (△) only the diagnosis count and names are provided (X)
33			Provision of detailed diagnosis results	whether detailed description of detected malicious codes and registries is provided (type, impact, risk, etc.)
34		Removal	Selective removal	whether users can selectively remove detected malicious codes and registries (O/X)
35		Log	Diagnosis and removal log	whether there is a diagnosis/removal log (O/X)
36		Recovery	Quarantine	whether a quarantine for managing infected items before removal is provided (O/X)
37	Performan	False alerts	Clean system false	whether files and registry entries are detected when the latest security update for

	ce		alerts	Windows XP Home SP3 (including Office 2003) is applied (O/X)
38		Removal	New malicious code sample removal rate	% of new malicious code files diagnosed and removed (0~100%)
39		Real-time	Malicious code real-time detection	whether malicious code files are detected at the same time as they are created or executed (O/X)

〈Attachment 3〉

Top programs in terms of malicious code removal rate (12)

(As of December 1, 2011)

Program name	Company name	charged/free
Daum Toolbar	Daum Communication	free
NoAd2+	MirageWorks	charged
V3 365 Clinic, V3 Lite	Ahn Lab	charged/free
Virus Chaser 8.0	SGA	free
Alyak 2.0	ESTSoft	free
nProtect AVS 3.0	Inca Internet	charged
ViRobot Internet Security 2011	Hauri	charged
My Family Doctor	KT	free service by ISP
U+ Internet PC Ansimmi	LG U+	charged service by ISP
Naver vaccine	NHN	free
B Internet Clean	SK Broadband	free service by ISP

※ Company names are in alphabetical order (Korean and English); charged/free classification is for personal users.

※ Programs that fail to meet essential requirements such as installation with consent and user agreement, or do not support real-time detection are excluded.

〈Attachment 4〉

Comparison of the results of the malicious code removal program investigation

Classification	Item		2010	2011	% change[1]
Customer support and program management items	Posted phone number		93.7% (193)	94.6% (191)	0.9%
	Answering of phone calls		70.4% (145)	56.9% (115)	-13.5%
	posted email		74.3% (153)	82.7% (167)	8.4%
	email reply		17.5% (36)	17.8% (36)	0.3%
	Bulletin board / FAQ		6.8% (14)	5.9% (12)	-0.9%
	Information related to e-commerce		53.4% (110)	58.4% (118)	5.0%
	Quality certification		6.8% (14)	7.4% (15)	0.6%
	Code signing		48.1% (99)	58.4% (118)	10.3%
	Website user agreement		92.7% (191)	90.6% (183)	-2.1%
	User agreement during installation		93.7% (193)	90.1% (182)	-3.6%
	Installation with consent		95.1% (196)	90.6% (183)	-4.5%
	Complete removal		78.6% (162)	81.7% (165)	3.1%
	Installation of additional programs		1.0% (2)	1.0% (2)	0.0%
	Automatic extension		68.0% (140)	72.8% (147)	4.8%
Program performance and functions	Automatic update		64.6% (133)	45.0% (91)	-19.6%
	Real-time surveillance		16.0% (33)	26.7% (54)	10.7%
	Quarantine		32.0% (66)	42.6% (86)	10.6%
	Provision of diagnosis details		90.3% (186)	82.2% (166)	-8.1%
	Selective removal		78.2% (161)	67.3% (136)	-10.9%
	Clean system false alerts		27.7% (57)	52.0% (105)	24.3%
	% removed	More than 2/3 (1,333 or 2,000)	17.5% (36)	31.2% (63)	13.7%
		10 ~ 2/3	10.2% (21)	20.8% (42)	10.6%
		1 ~ 10	1.5% (3)	2.0% (4)	0.5%
		0	64.1% (132)	38.6% (78)	-25.5%
		Unable to check[2] (abnormal operation)	6.8% (14)	7.4% (15)	0.6%

1) Change: 2011 ratio − 2010 ratio

2) Reason for inability to check: inability to download, service stop, installation and execution errors, etc.

〈Attachment 5〉

10 rules of using vaccine programs

<10 rules of using vaccine programs>

□ **Selection and installation of excellent vaccine programs**

① Select excellent vaccines chosen by the Domestic Malicious Code Removal Program Investigation

※ (excellent programs chosen by the investigation) http://www.boho.or.kr/vaccine.jsp

② Install the vaccine only from the official website of the company

③ Exercise caution with regard to vaccine programs installed as a tie-in for other software

□ **Correct utilization of the vaccine program detection/removal function**

④ Keep the vaccine up-to-date, and check periodically

⑤ Have real-time detection turned on at all times

□ **How to deal with faulty vaccine programs enticing users to make a payment**

⑥ Delete the vaccine program that you don't use when it asks you to pay after automatic diagnosis

⑦ If requested to make a payment, check the detailed agreement thoroughly including automatic payment extension.

⑧ Check the monthly automatic transfer bill, and terminate vaccine programs that you don’t use.

□ **How to respond to vaccine programs through related agencies**

⑨ If vaccine programs are not deleted, call the KISA 118 counseling service.

※ Korea Internet Security Agency 118 Center (118, www.boho.or.kr)

⑩ If you suffer damages in relation to a vaccine, call the 1372 Consumer Consultation Center or the cell phone/ARS S-payment.

※ 1372 Consumer Counseling Center (1372, www.ccn.go.kr)

※ Cell phone/ARS Spayment (www.spayment.org: homepage)