Security Trend

ASEC REPORT

VOL.53
May, 2014

AhnLab

ASEC REPORT

VOL.53 May, 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 MAY 2014

Table of Contents

1 SECURITY STATISTICS

2 SECURITY ISSUE

1

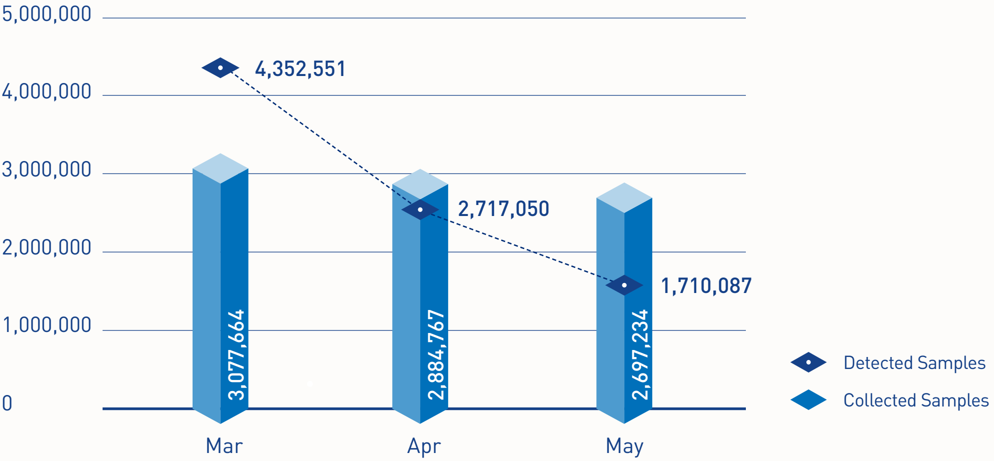
SECURITY STATISTICS

SECURITY STATISTICS

01

Malware Statistics

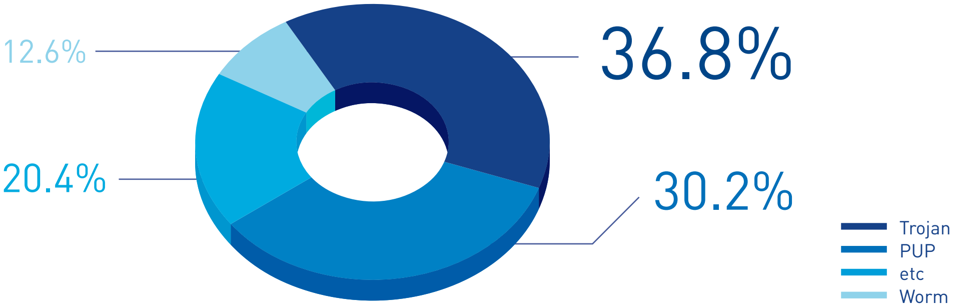
According to the ASEC (AhnLab Security Emergency Response Center), 1,710,187 malware were detected in May 2014. The number of detected malware decreased by 1,006,963 from 2,717,050 detected in the previous month as shown in Figure 1-1. A total of 2,697,234 malware samples were collected in May.



[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 May 2014. It appears that Trojans was the most distributed malware with 36.8% of the total. It was followed by PUP (30.2%) and Worm (12.6%).



[Figure 1-2] Proportion of Malware Type in May

Table 1-1 shows the Top 10 malware threats in May categorized by malicious code name. PUP/Win32.IntClient was the most frequently detected malware (148,164), followed by Trojan/Win32.Agent (87,720).

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

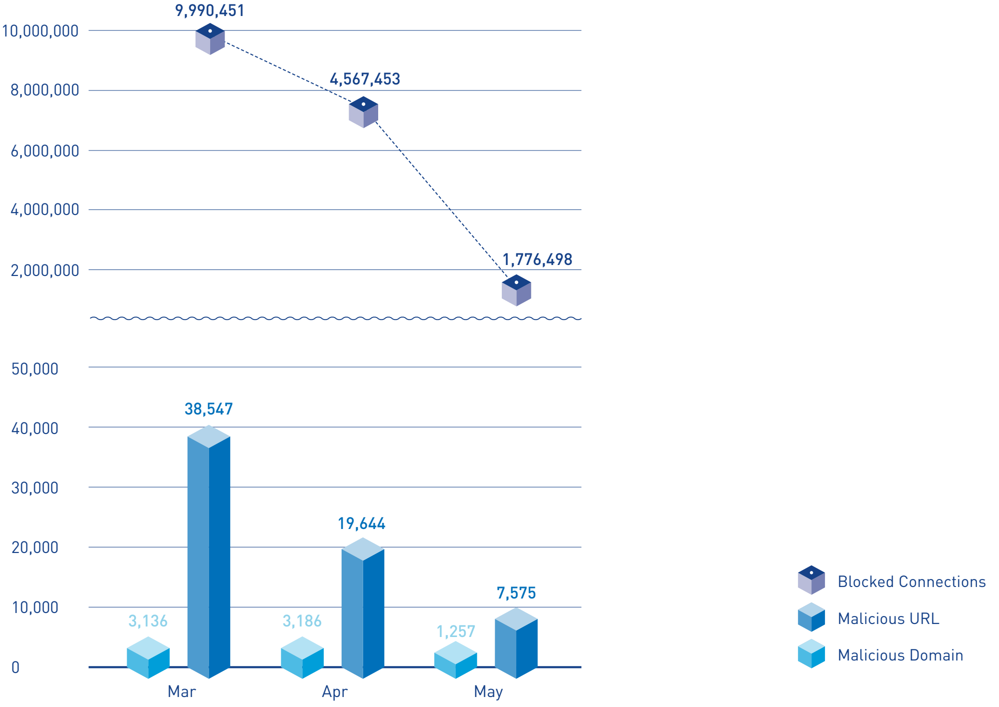
Rank	Malicious code name	No. of detection
1	PUP/Win32.IntClient	148,164
2	Trojan/Win32.Agent	87,720
3	PUP/Win32.GearExt	56,913
4	PUP/Win32.Kraddare	46,728
5	Trojan/Win32.Hupe	42,543
6	Trojan/Win32.OnlineGameHack	41,662
7	Trojan/Win32.Gen	38,430
8	ASD.Prevention	37,111
9	Unwanted/Win32.Agent	35,405
10	Trojan/Win32.Downloader	34,071

SECURITY STATISTICS

02

Web Security Statistics

In May 2014, a total of 7,575 domains and 1,257 URLs were comprised and used to distribute malware. In addition, 1,776,498 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.



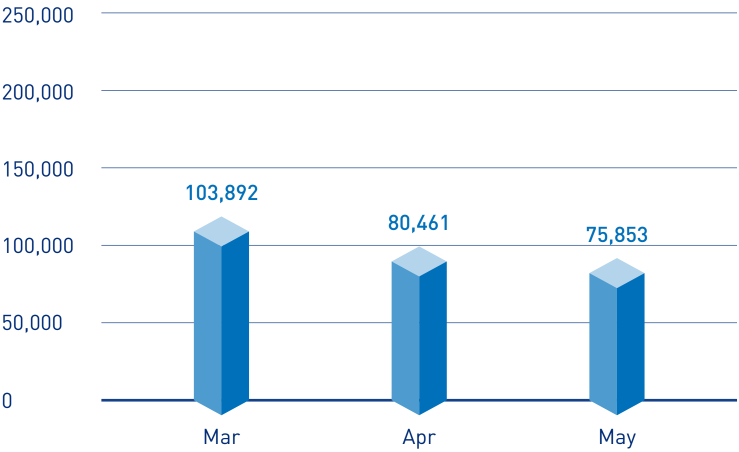
[Figure 1-3] Malicious Domains/URLs Trend

SECURITY STATISTICS

03

Mobile Malware Statistics

In May 2014, 75,853 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 in May 2014 categorized by malicious code name. Malicious applications that were disguised as installation programs continue to be frequently detected, such as Android-Trojan/FakeInst. Thus, it is advised that users exercise cautious when using mobile applications or the internet via mobile phones.

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

Rank	Malicious code name	No. of detection
1	Android-Trojan/FakeInst	18,801
2	Android-PUP/Dowgin	16,830
3	Android-PUP/Wapsx	4,625
4	Android-Trojan/Opfake	3,713
5	Android-Trojan/SMSAgent	1,685
6	Android-Trojan/Mseg	1,233
7	Android-Trojan/SmsSend	1,129
8	Android-PUP/SMSreg	1,094
9	Android-PUP/Kuguo	1,074
10	Android-PUP/Admogo	1,060

2

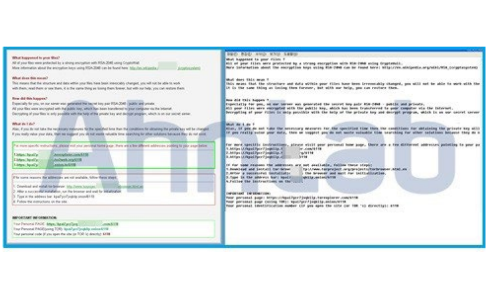
SECURITY ISSUE

Ransomware, the Kryptonite of PC files?

Ransomware, the Kryptonite of PC files?

Ransomware limits the usability of user devices through several methods that coerce the user into paying a ransom.

A recently discovered ransomware called "CryptoWall" spread via email and currently encrypts the files of a great number of users, using it as a way to demand payment.



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia/[redacted]_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1.https://kpai7y[redacted].torexplorer.com/6118
2.https://kpai7y[redacted].tor2web.org/6118
3.https://kpai7y[redacted].onion.to/6118

If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.[redacted]/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: kpai7ycr7jxqkilp.onion/6118
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your Personal PAGE: https://kpai7ycr7jxq[redacted].com/6118
Your Personal PAGE(using TOR): kpai7ycr7jxqkilp.onion/6118
Your personal code (if you open the site (or TOR 's) directly): 6118

What happened to your files ?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean ?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with the
it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen ?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server

What do I do ?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do n

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your pa
1.https://kpai7ycr7jxqkilp.[redacted]r.com/6118
2.https://kpai7ycr7jxqkilp.[redacted]rg/6118
3.https://kpai7ycr7jxqkilp.[redacted]/6118

If for some reasons the addresses are not available, follow these steps:
1.Download and install tor-brows[redacted]tp://www.torproject.org/projects/torbrowser.html.en
2.After a successful installati[redacted] the browser and wait for initialization.
3.Type in the address bar: kpai[redacted]qkilp.onion/6118
4.Follow the instructions on the [redacted]

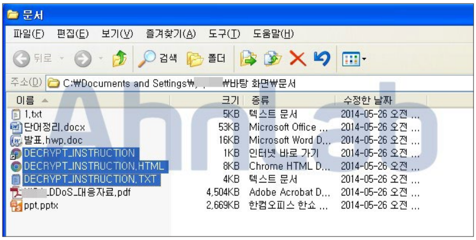
IMPORTANT INFORMATION:
Your personal page: https://kpai7ycr7jxqkilp.torexplorer.com/6118
Your personal page (using TOR): kpai7ycr7jxqkilp.onion/6118
Your personal identification number (if you open the site (or TOR 's) directly): 6118

Figure 2-1 | Screen appearing upon a CryptoWall infection

When infected by CryptoWall, several extension files (*.doc, *.docx, *.xls, *.ppt, *.psd, *.pdf, *.eps, *.ai, *.cdr, *.jpg, etc.) are encrypted through the algorithm RSA-2048, and screen is displayed to the user as seen in Figure 2-1. The user is given a detailed explanation as to what the algorithm RSA-2048 is, its restoration method, and what the user needs to do in order to restore the files. Afterwards, the attacker demands payment for its services.

If a PC containing important business or personal documents should become infected by CryptoWall, it can lead to serious consequences. In this way, malware creators are taking advantage of users' willingness to restore files even at monetary cost.

A CryptoWall infection creates the three files shown in Figure 2-2 in the path of every encrypted file.



문서

주소(D) C:₩Documents and Settings₩[redacted]₩바탕 화면₩문서

이름	크기	종류	수정한 날짜
1.txt	5KB	텍스트 문서	2014-05-26 오전 ...
단어정리.docx	53KB	Microsoft Office ...	2014-05-26 오전 ...
발표.hwp.doc	16KB	Microsoft Word D...	2014-05-26 오전 ...
DECRYPT_INSTRUCTION	1KB	인터넷 바로 가기	2014-05-26 오전 ...
DECRYPT_INSTRUCTION.HTML	8KB	Chrome HTML D...	2014-05-26 오전 ...
DECRYPT_INSTRUCTION.TXT	4KB	텍스트 문서	2014-05-26 오전 ...
[redacted]_DDoS_대응자료.pdf	4,504KB	Adobe Acrobat D...	2014-05-26 오전 ...
ppt.pptx	2,669KB	한컴오피스 한쇼 ...	2014-05-26 오전 ...

Figure 2-2 | Files created upon infection

These three files contain the same message as the one displayed when infected.

Opening a file encrypted by the malware will display a pop-up message indicating that the file is compromised. Even if the file opens, it will be filled with scrambled text, as shown in Figure 2-3.

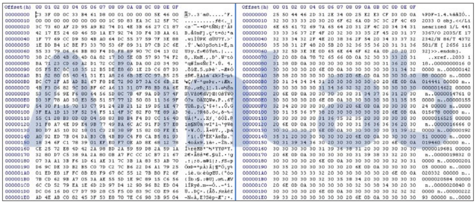
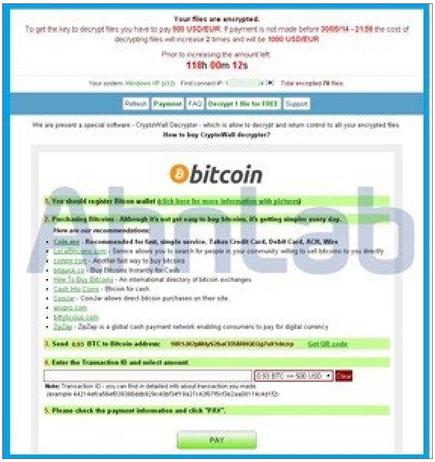


Figure 2-3 | Encrypted PDF file (left)
Normal PDF file (right)

Unlike normal PDF files, all data in an infected file is encrypted by the algorithm RSA-2048. Therefore, the file cannot be read without a decryption key.



Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 30/05/14 - 21:58 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:

118h 00m 12s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 78 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcoin wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- Coinbase - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- coinrnr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bitcoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency

3. Send [illegible] BTC to Bitcoin address: [illegible] Get QR code
4. Enter the Transaction ID and select amount:

[illegible] BTC == 500 USD ▾ Clear

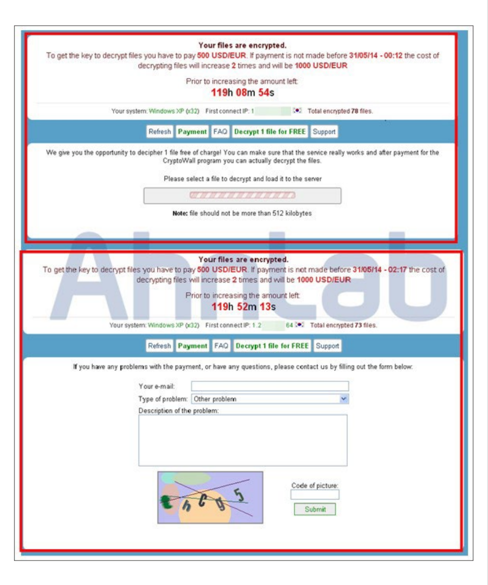
Note: Transaction ID - you can find in detailed info about transaction you made. (example [illegible])

5. Please check the payment information and click "PAY".

Figure 2-4 | Page demanding Bitcoin payment

Like most ransomware, the CryptoWall increases the ransom demanded if it is not paid within an indicated period. It also displays a message to the user saying that the decryption key will be deleted, thus making the infected file permanently unrecoverable. This interferes with a user's rational judgment and induces payment. Also, setting a deadline for payment effectively invokes a sense of urgency in the user

As reassurance, a single encrypted file is decrypted to show the user that decryption of all files is indeed possible if a payment of $500 is made.



Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 31/05/14 - 00:12 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:
119h 08m 54s

Your system: Windows XP (x32) First connect IP: 1 Total encrypted 78 files.

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

Please select a file to decrypt and load it to the server

Note: file should not be more than 512 kilobytes

Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 31/05/14 - 02:17 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:
119h 52m 13s

Your system: Windows XP (x32) First connect IP: 1.2 64 Total encrypted 73 files.

If you have any problems with the payment, or have any questions, please contact us by filling out the form below:

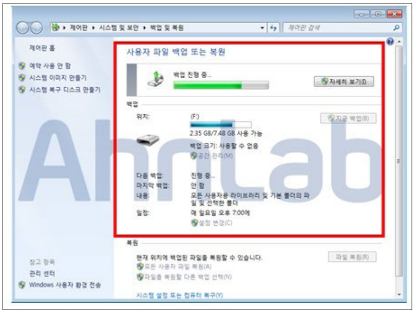
Your e-mail:
Type of problem: Other problem
Description of the problem:

Code of picture:

Figure 2-5 | Sample file decryption window (top)
User support (bottom)

As can be seen in Figure 2-5, CryptoWall comes with a user support function that allows communication between the user (buyer) and attacker (seller). It appears that the attacker tries to reassure the user and persuade him or her to make payment by providing a detailed explanation and decrypting one file as a sample. Security researchers at the ASEC (AhnLab Security Emergency Response Center) attempted to contact the attacker through this function, but received no response.

It seems almost impossible to restore the encrypted files by ransomware unless a ransom is paid. In the meantime, it is not guaranteed that all files will be restored even if the user pays the ransom. Thus, the best measure is for users to take precautions for their files in their PCs before being unexpectedly encrypted by ransomware. For example, it is recommended to back up important documents and files as a preventive measure. You can use the user file backup function in Windows to minimize damage. Even after a CryptoWall infection, encrypted files can be restored if a restore point has been set or if they have been backed up.



제어판 ▸ 시스템 및 보안 ▸ 백업 및 복원

사용자 파일 백업 또는 복원

백업 진행 중...

백업

위치: (F:)
2.35 GB/7.48 GB 사용 가능
백업 크기: 사용할 수 없음

다음 백업: 진행 중...
마지막 백업: 안 함
내용: 모든 사용자용 라이브러리 및 기본 폴더의 파일 및 선택한 폴더
일정: 매 일요일 오후 7:00에

복원

현재 위치에 백업된 파일을 복원할 수 있습니다.

Figure 2-6 | User file backup

In order to successfully restore backed up files, it is critical that the files are not backed up to the local disk where Windows is installed, but to another storage device. A local disk is not displayed in the path where a backup file is to be saved, and the user is able to designate the file or folder to be backed up on a local disk.

Backed up files can be restored by overwriting them onto the original files or saving them to a path different from the original one. AhnLab has verified that files backed up this way can be restored to a designated path and successfully executed.

V3 detects the relevant malware as follows.

< Malicious code name in V3 products>

Trojan/Win32.Agent (2013.05.07.00)

AhnLab

ASEC REPORT VOL.53
May, 2014

Contributors ASEC Researchers
Editor Content Creatives Team
Design UX Design Team

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