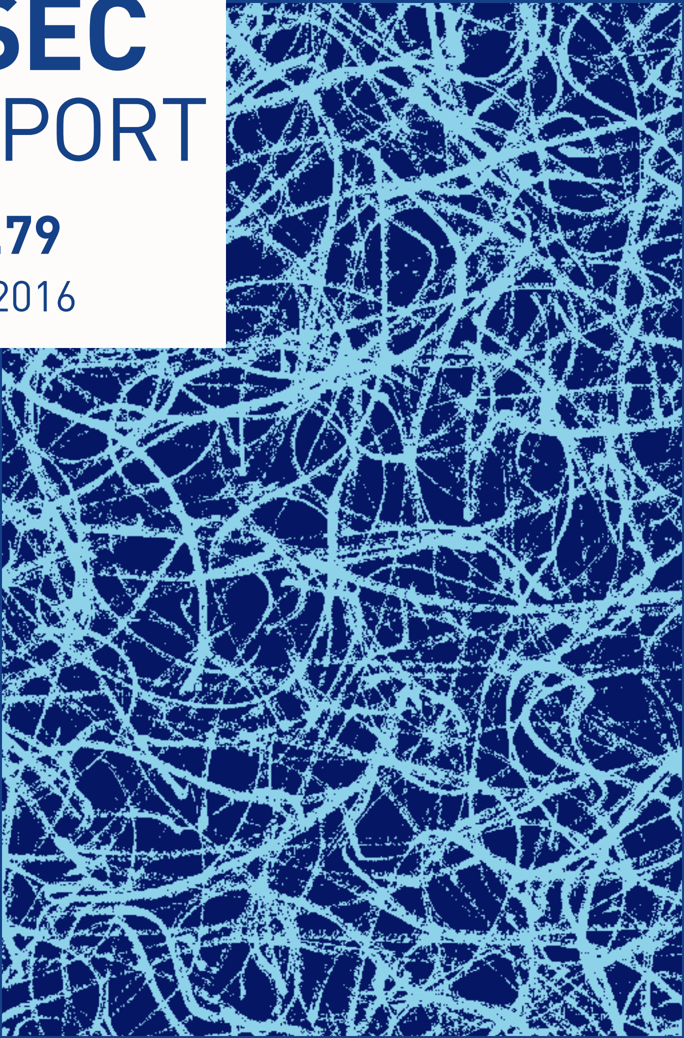
Security Trend

ASEC REPORT

VOL.79

July, 2016



AhnLab

ASEC REPORT

VOL.79 July, 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 July 2016

Table of Contents

1

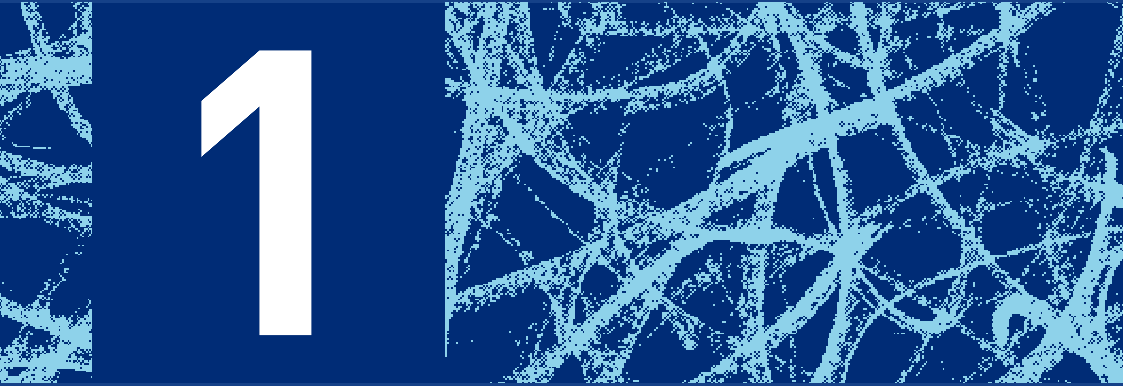
SECURITY STATISTICS

2

SECURITY ISSUE

3

IN-DEPTH ANALYSIS



1

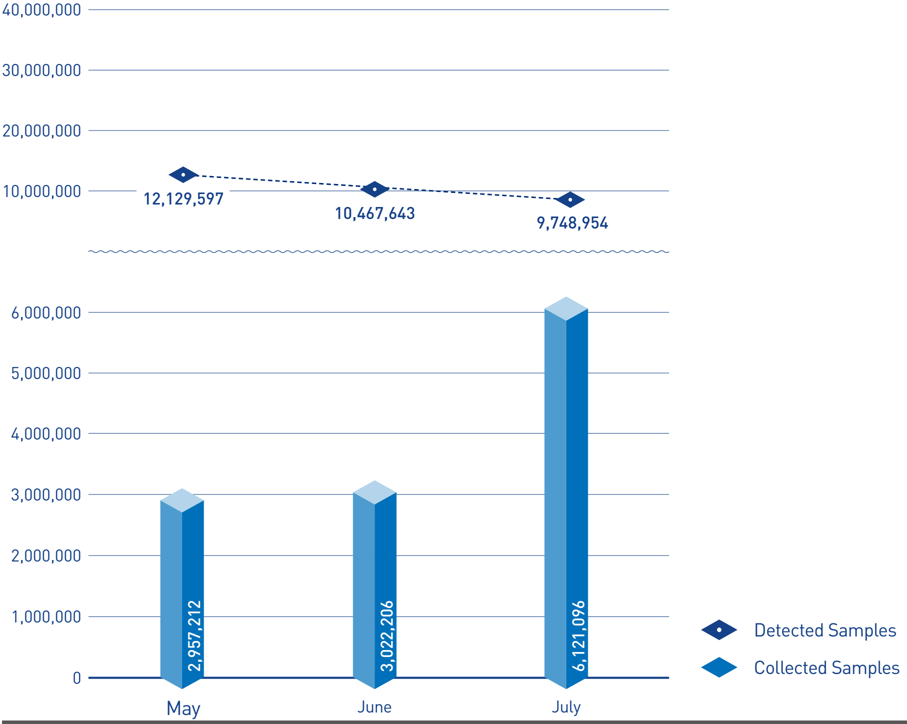
SECURITY STATISTICS

SECURITY STATISTICS

01

Malware Statistics

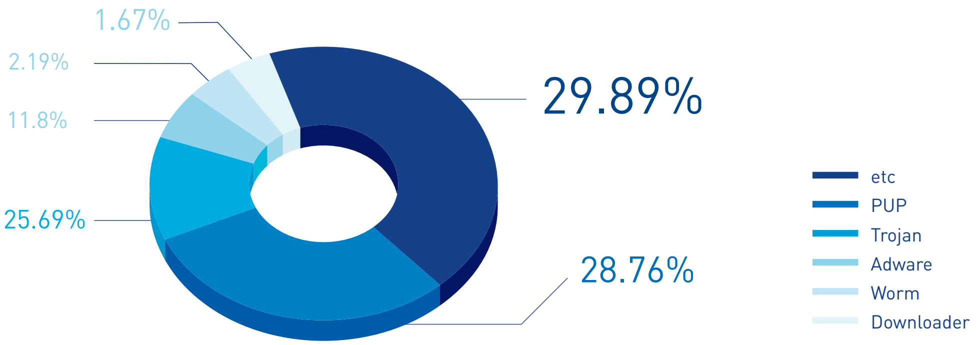
According to the ASEC (AhnLab Security Emergency Response Center), 9,748,954 malware were detected in July 2016. The number of detected malware decreased by 718,689 from 10,467,643 detected in the previous month as shown in Figure 1-1. A total of 6,121,096 malware samples were collected in July.



[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 July 2016. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 28.76% of the total. It was followed by Trojan (25.69%) and Worm (2.19%).



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

Table 1-1 shows the Top 10 malware threats in July categorized by alias. Malware/Win32.Generic was the most frequently detected malware (364,815), followed by Trojan/Win32.Starter (179,373).

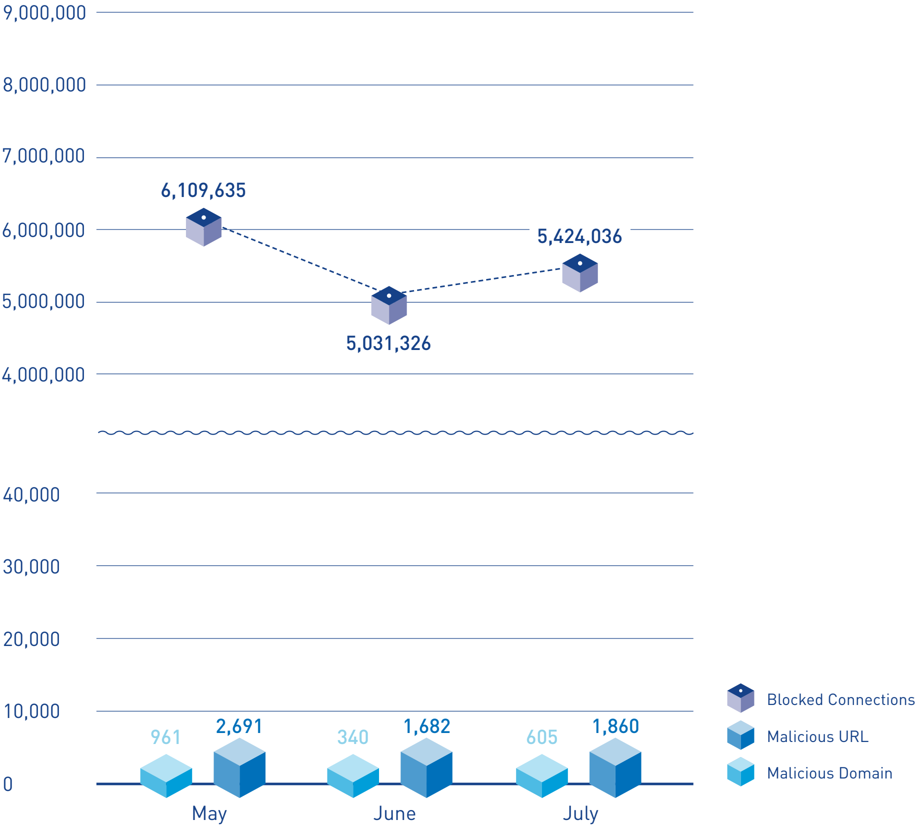
[Table 1-1] Top 10 Malware Threats in July 2016 (by Alias)

Rank	Alias from AhnLab	No. of detections
1	Malware/Win32.Generic	364,815
2	Trojan/Win32.Starter	179,373
3	Unwanted/Win32.HackTool	110,173
4	Trojan/Win32.Agent	78,755
5	Trojan/Win32.Neshta	70,323
6	HackTool/Win32.Crack	68,710
7	Trojan/Win32.CryptXXX	65,758
8	Trojan/Win32.Cerber	57,281
9	ASD.Prevention	54,878
10	Unwanted/Win32.Keygen	53,390

02

Web Security Statistics

In July 2016, a total of 605 domains and 1,860 URLs were comprised and used to distribute malware. In addition, 5,424,036 malicious domains and URLs were blocked.



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

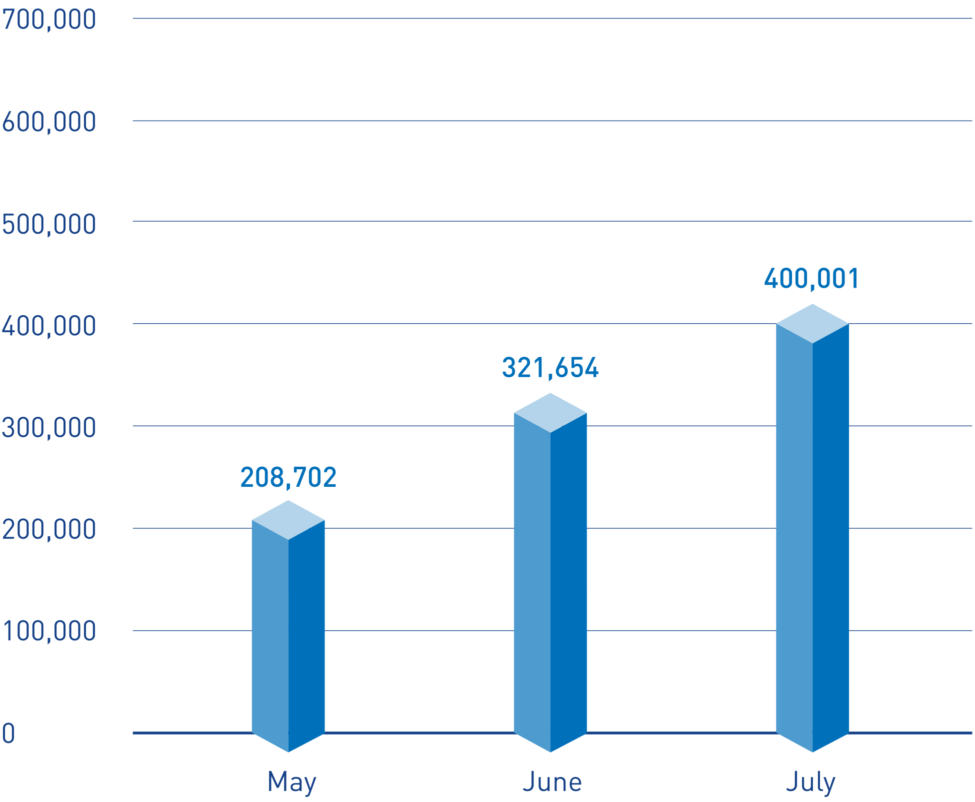
* "Blocked Connections" refers to the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers.

SECURITY STATISTICS

03

Mobile Malware Statistics

In July 2016, 400,001 mobile malware were detected as shown in Figure 1-4.



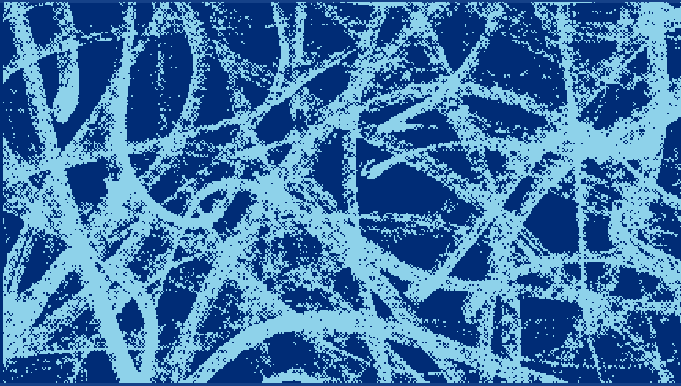
[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in July 2016. Android-PUP/SmsPay was the most distributed malware with 81,588 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	81,588
2	Android-PUP/Shedun	58,123
3	Android-PUP/SmsReg	33,097
4	Android-PUP/Zdpay	26,288
5	Android-PUP/Noico	20,338
6	Android-PUP/Dowgin	17,879
7	Android-Trojan/Hidap	12,051
8	Android-Trojan/Agent	11,063
9	Android-Trojan/Moavt	10,598
10	Android-Trojan/AutoSMS	8,752

2



SECURITY ISSUE

Pokémon GO! Malware Go?!

SECURITY ISSUE

Pokémon GO! Malware Go?!

With the popularity of Pokémon GO exploding across the world, more incidents involving users of the augmented reality (AR) game are being reported daily. Recently, users are being urged to exercise caution after the discovery of malware buried in installation files of the game that is being distributed via channels outside the official application store.

TAKE POKÉMON PHOTOS!

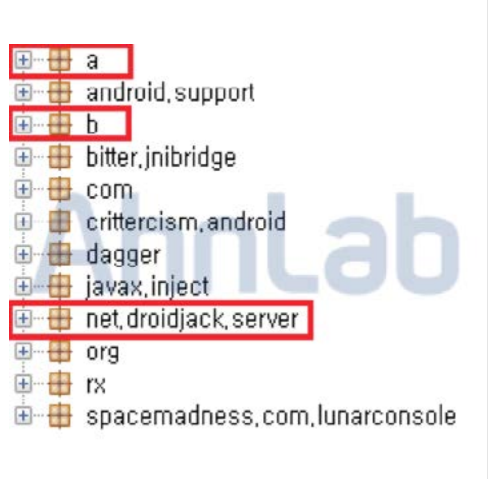
Snap photos of Pokémon with Pokémon GO! When you encounter a wild Pokémon, you can enable a view that uses the camera on your smartphone to display real-life surroundings as the background, making it appear as if the Pokémon is with you in the real world!

You can also quickly select a camera that is conveniently stored in your inventory to snap a photo of the Pokémon on screen. The photo is stored on your device, making it very easy to share with friends.

Always be careful when taking a photo to make sure everyone in the photo is OK with having their picture taken and that there's nothing personal in the photo you don't want to share.

Figure 2-1 | Pokémon Go official Web page (http://www.pokemongo.com)

Pokémon GO was released first in the United States and Austria on July 6 and rolled out across a total of 35 countries around the world. Users in South Korea and other countries where the game has not been official released yet, however, are still playing it by downloading the APK file from websites. Attackers are taking advantage of this workaround to plant and distribute malware.



```
a
android.support
b
bitter.jnibridge
com
crittercism.android
dagger
javax.inject
net.droidjack.server
org
rx
spacemadness.com.lunarconsole
```

Figure 2-2 | Abnormal class files added in a normal APK file

The recently-discovered malicious APK file does in fact install a copy of the Pokémon GO game but also contains class files that hold malicious functions designed to extract the infected smart phone's information as shown in Figure 2-2. A check of the internal package names reveals a remote access trojan

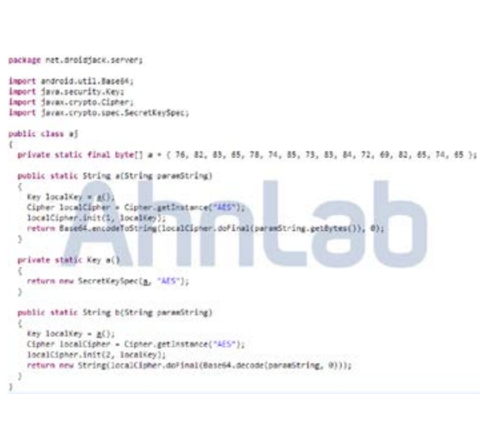
(RAT) called DroidJack, a hacking tool that allows an attacker to remotely control an infected Android smart phone.

When a user installs a new app, the malicious Pokémon GO demands permissions unrelated to the game such as SMS, phone and recording functions, thereby gaining access to the smart phone's internal information.

Table 2-1 | User information obtained by the Pokémon GO malware

- Hijack SMS
- Hijack contact list
- Hijack call history
- Hijack GPS information
- Hijack files stored in the phone
- Run and control applications
- Eavesdropping and recording via the phone's mic

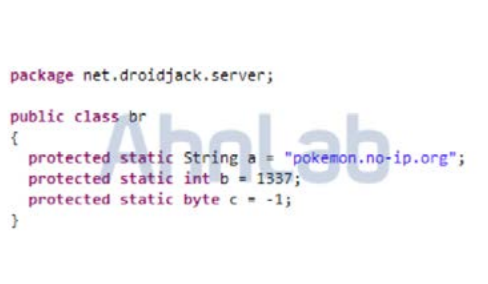
The attacker hijacks user information from the smart phone infected with the malware disguised as Pokémon GO as shown in Table 2-1, and remotely control the phone's system.



```
package net.droidjack.server;

import android.util.Base64;
import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

public class aj
{
  private static final byte[] a = { 76, 82, 83, 65, 78, 74, 85, 73, 83, 84, 72, 69, 82, 65, 74, 65 };

  public static String a(String paramString)
  {
    Key localKey = a();
    Cipher localCipher = Cipher.getInstance("AES");
    localCipher.init(1, localKey);
    return Base64.encodeToString(localCipher.doFinal(paramString.getBytes()), 0);
  }

  private static Key a()
  {
    return new SecretKeySpec(a, "AES");
  }

  public static String b(String paramString)
  {
    Key localKey = a();
    Cipher localCipher = Cipher.getInstance("AES");
    localCipher.init(2, localKey);
    return new String(localCipher.doFinal(Base64.decode(paramString, 0)));
  }
}
```

Figure 2-3 | Encrypts stolen data

The information hijacked from the phone is encrypted as shown in Figure 2-3 before being sent to a C&C server. The DroidJack console eventually allows the attacker to easily extract these and other information from the infected phone.



```
package net.droidjack.server;

public class br
{
  protected static String a = "pokemon.no-ip.org";
  protected static int b = 1337;
  protected static byte c = -1;
}
```

Figure 2-4 | C&C addresses accessed by the malware

The rising popularity of Pokémon GO is leading to an increase in incidences of attacks and cyber crimes using malicious APKs disguised as the game and targeting users in regions where Pokémon GO has not yet officially been released. Smart phone users should always use the official app store when downloading and installing new apps, and avoid installing APK files whose origins may be suspect and integrity unverified.

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

<Alias identified by V3 products>

Android-Trojan/Sandrorat (2015.01.17.01)

3

IN-DEPTH ANALYSIS

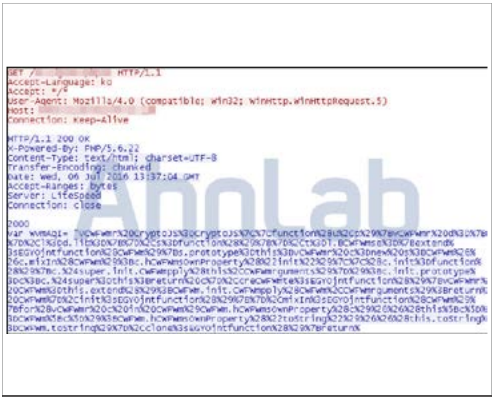
Ransomware disguised as shortcut files (.LNK) uncovered

IN-DEPTH ANALYSIS

Ransomware disguised as shortcut files (.LNK) uncovered

With the ransomware threat wave showing no signs of easing off, a new type of ransomware that disguises itself using the extension for a shortcut file (*.LNK) has been identified. A Windows shortcut is a file that contains the path of the relevant file, designed to allow the use of parameters for the program to be executed. A string can be inserted into the parameters to enable the shortcut to perform certain functions, and malware that takes advantage of this feature has recently been on the rise.

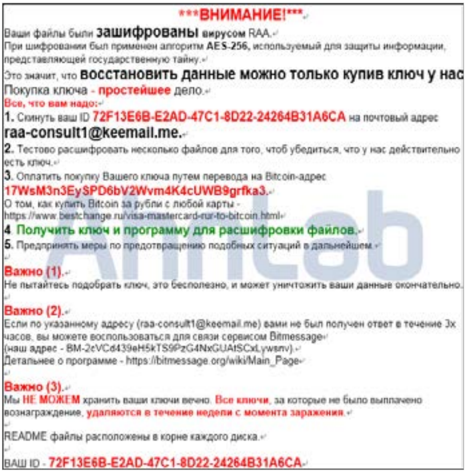
The latest iteration of this malware also exploits this feature of shortcut (.LNK) files. The ransomware, which has been distributed as a shortcut file, inserts a JavaScript source into the command prompt (cmd.exe) to run the malicious script, which then accesses a certain URL to receive the string of text.



```
GET /[redacted] HTTP/1.1
Accept-Language: ko
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: [redacted]
Connection: Keep-Alive

HTTP/1.1 200 OK
X-Powered-By: PHP/5.6.22
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 06 Jul 2016 13:37:04 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close

2000
var wvmAqi= "vCWFwmr%20CryptoJS%3DCryptoJS%7C%7Cfunction%28u%2Cp%29%7BvCWFwmr%20d%3D%7B
%7D%2Cl%3Dd.lib%3D%7B%7D%2Cs%3Dfunction%28%29%7B%7D%2Ct%3Dl.BCWFwmse%3D%7Bextend%
3sEGYOjntfunction%28CWFwm%29%7Bs.prototype%3Dthis%3BvCWFwmr%20c%3Dnew%20s%3BCWFwm%26%
26c.mixIn%28CWFwm%29%3Bc.hCWFwmsOwnProperty%28%22init%22%29%7C%7C%28c.init%3Dfunction%
28%29%7Bc.%24super.init.CWFwmpply%28this%2CCWFwmrguments%29%7D%29%3Bc.init.prototype%
3Dc%3Bc.%24super%3Dthis%3Breturn%20c%7D%2Ccre@CWFwmte%3sEGYOjntfunction%28%29%7BvCWFwmr%
20CWFwm%3Dthis.extend%28%29%3BCWFwm.init.CWFwmpply%28CWFwm%2CCWFwmrguments%29%3Breturn%
20CWFwm%7D%2Cinit%3sEGYOjntfunction%28%29%7B%7D%2CmixIn%3sEGYOjntfunction%28CWFwm%29%
7Bfor%28vCWFwmr%20c%20in%20CWFwm%29CWFwm.hCWFwmsOwnProperty%28c%29%26%26%28this%5Bc%5D%
3DCWFwm%5Bc%5D%29%3BCWFwm.hCWFwmsOwnProperty%28%22toString%22%29%26%26%28this.toString%
3DCWFwm.toString%29%7D%2Cclone%3sEGYOjntfunction%28%29%7Breturn%
```

Figure 3-1 | Text string received

The text, as shown in Figure 3-1, reveals itself to be the malicious code of a ransomware designed in JavaScript. The malicious script file is executed using wscript.exe, a windows application. When the scrip is run, the ransomware encrypts the user's files and outputs a notice, shown in Figure 3-2, demanding payment in return for restoring the encrypted files.



ВНИМАНИЕ!
Ваши файлы были **зашифрованы** вирусом RAA.
При шифровании был применен алгоритм **AES-256**, используемый для защиты информации, представляющей государственную тайну.
Это значит, что **восстановить данные можно только купив ключ у нас**
Покупка ключа - **простейшее** дело.
Все, что вам надо:
1. Скинуть ваш ID **72F13E6B-E2AD-47C1-8D22-24264B31A6CA** на почтовый адрес
raa-consult1@keemail.me.
2. Тестово расшифровать несколько файлов для того, чтоб убедиться, что у нас действительно есть ключ.
3. Оплатить покупку Вашего ключа путем перевода на Bitcoin-адрес
17WsM3n3EySPD6bV2Wvm4K4cUWB9grfka3.
О том, как купить Bitcoin за рубли с любой карты -
https://www.bestchange.ru/visa-mastercard-rur-to-bitcoin.html
4. **Получить ключ и программу для расшифровки файлов.**
5. Предпринять меры по предотвращению подобных ситуаций в дальнейшем.

Важно (1).
Не пытайтесь подобрать ключ, это бесполезно, и может уничтожить ваши данные окончательно.

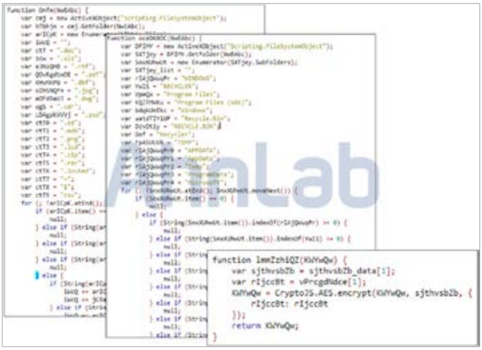
Важно (2).
Если по указанному адресу (raa-consult1@keemail.me) вами не был получен ответ в течение 3х часов, вы можете воспользоваться для связи сервисом Bitmessage
(наш адрес - BM-2cVCd439eH5kTS9PzG4NxGUAtSCxLywsnv).
Детальнее о программе - https://bitmessage.org/wiki/Main_Page

Важно (3).
Мы **НЕ МОЖЕМ** хранить ваши ключи вечно. **Все ключи**, за которые не было выплачено вознаграждение, **удаляются в течение недели с момента заражения.**

README файлы расположены в корне каждого диска.

ВАШ ID - **72F13E6B-E2AD-47C1-8D22-24264B31A6CA**

Figure 3-2 | Pay-up warning dialogue of the ransomware



```
function Onfe(NwEAbc) {
    var cmj = new ActiveXObject("Scripting.FileSystemObject");
    var hTbhjn = cmj.GetFolder(NwEAbc);
    var arICpK = new Enumera
    var lmcQ = "";
    var ctT = ".doc";
    var hOw = ".xls";
    var eJNsQHB = ".rtf";
    var QOvAgpDxOE = ".pdf";
    var KMnFRPB = ".dbf";
    var eIMVANQPe = ".jpg";
    var mOFdDaCI = ".dwg";
    var ogb = ".cdr";
    var LDAgpRVVVJ = ".psd";
    var ctT0 = ".cd";
    var ctT1 = ".mdb";
    var ctT2 = ".png";
    var ctT3 = ".lcd";
    var ctT4 = ".zip";
    var ctT5 = ".rar";
    var ctT6 = ".locked";
    var ctT7 = "~";
    var ctT8 = "$";
    var ctT9 = ".csv";
    for (; !arICpK.atEnd();
        if (arICpK.item() ==
            null;
        } else if (String(ar
            null;
        } else if (String(ar
            null;
        } else if (String(ar
            null;
        } else {
            if (String(arICa
                lmcQ == arI
                lmcQ == jCKa
            } else if (Strin
```

```
function ocWOXBOX(NwEAbc) {
    var DFIHY = new ActiveXObject("Scripting.FileSystemObject");
    var SXTjey = DFIHY.GetFolder(NwEAbc);
    var SnoXURwUR = new Enumerator(SXTjey.SubFolders);
    var SXTjey_list = "";
    var rIAJQuupPr = "WINDOWS";
    var YwIS = "RECYCLER";
    var VpmQx = "Program Files";
    var KQJTMWKu = "Program Files (x86)";
    var bdqkUmEkc = "Windows";
    var amldTIYIGP = "Recycle.Bin";
    var DUvOtIj = "RECYCLE.BIN";
    var Dmf = "Recycler";
    var FpAXUUUR = "TEMP";
    var rIAJQuupPr0 = "APPDATA";
    var rIAJQuupPr1 = "AppData";
    var rIAJQuupPr2 = "Temp";
    var rIAJQuupPr3 = "ProgramData";
    var rIAJQuupPr4 = "Microsoft";
    for (; !SnoXURwUR.atEnd(); SnoXURwUR.moveNext()) {
        if (SnoXURwUR.item() == 0) {
            null;
        } else {
            if (String(SnoXURwUR.item()).indexOf(rIAJQuupPr) == 0) {
                null;
            } else if (String(SnoXURwUR.item()).indexOf(YwIS) == 0) {
                null;
            } else if (Strin
                null;
            } else if (Strin
                null;
            } else if (Strin
                null;
            } else if (Strin
                null;
            } else if (Strin
```

```
function lmmZzhiQZ(KWYwQw) {
    var sjthvsbZb = sjthvsbZb_data[1];
    var rIjccBt = vPrcgdNdce[1];
    KWYwQw = CryptoJS.AES.encrypt(KWYwQw, sjthvsbZb, {
        rIjccBt: rIjccBt
    });
    return KWYwQw;
}
```

Figure 3-3 | Obfuscated malicious script

The downloaded malicious script is obfuscated to evade analysis as shown in Figure 3-3, and encrypts the system's files using the AES algorithm of CryptoJS, an encryption library. File extensions that are targeted for encryption are shown in Table 3-1.

Table 3-1 | File extensions targeted for encryption

.doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr,
.psd, .cd, .mdb, .png, .lcd, .zip, .rar, .csv

While most ransomware discovered to date use malicious script files in *.js, *.vbs or *.wsf formats or document files embedded with malicious macros, the recently-discovered ransomware uses the inherent vulnerability of shortcut files (*.LNK) to download and run a malicious script. This requires users to be especially con guard, since the malware uploaded to the server can take the form of other types of malware in addition to ransomware capable of causing additional serious damage to the system.

Perpetrators of malware attacks are spreading increasingly advanced ransomware via a variety of channels. To protect against the threat of ransomware, security updates should be installed to prevent drive-by-download attacks and anti-virus program engines should always be kept up to date. Backing up import files would also be prudent.

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

<Aliases identified by V3 products>
VBS/Raalocker (2016.07.07.04)
LNK/Downloader (2016.07.07.09)

AhnLab

ASEC REPORT VOL.79
July, 2016

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