MALWARE ANALYSIS REPORT

NotCompatible – Android Web Proxy Bot

Alcatel·Lucent

TABLE OF CONTENTS

SUMMARY

This paper analyzes in details the "NotCompatible" android malware and brings evidence that mobile devices will get more and more infected in a near future, leveraging systems already used on the fixed side. Moreover, NotCompatible is a threat for both users and network operators as it consumes a lot bandwidth and airtime.

It is an Android bot that uses the infected phone as a proxy for this illicit web browsing activity. The command and control servers (C&C) are located in Germany and Holland. The protocol is the same as a Windows based web proxy bot. This is the first time we've seen a common C&C infrastructure shared between Windows and Android malware. The malware was first discovered in early 2012 and has had a recent resurgence due to a spam campaign to spread the malware.

There are some interesting aspects of NotCompatible that makes it stand out from other Android malware:

- It can **consume considerable network resources** and will likely lead to large data charges, particularly for roaming users. In one instance, we saw an infected phone consuming 165 Mbytes of web bandwidth in less than two hours across over 300 K TCP flows. Almost all of this activity can be attributed to the web-proxy activity.
- The C&C and the network servers that support it are same as one used by Windows malware that provides the same proxy services. **This is the first time we've seen both Windows PCs and Android phones operating as a single botnet.**
- A spam based phishing attack lures users to infected web sites that automatically download the file Update.apk to the phone. The user must click "install" for the installation to proceed.
- The infection rate from the field shows that 0.03% of mobile devices are infected. This may not seem like much, but the bandwidth consumption can add up. For example in a mobile network with 1 M devices, 300 will be infected and would consume a total of **720 GBytes of data per day**.

MALWARE SAMPLE

We have a number of samples of NotCompatible. We chose the following because it had generated a good quantity of network traffic for analysis.

VID: 11219849
MD5: 0e8525862f9c98d2de42042718f563fe
Size: 14030 bytes
Source: Indusface
File Type: Android Application
Sample Collected: 2013-03-23 11:53:06
Sample Inserted: 2013-03-23 11:53:06

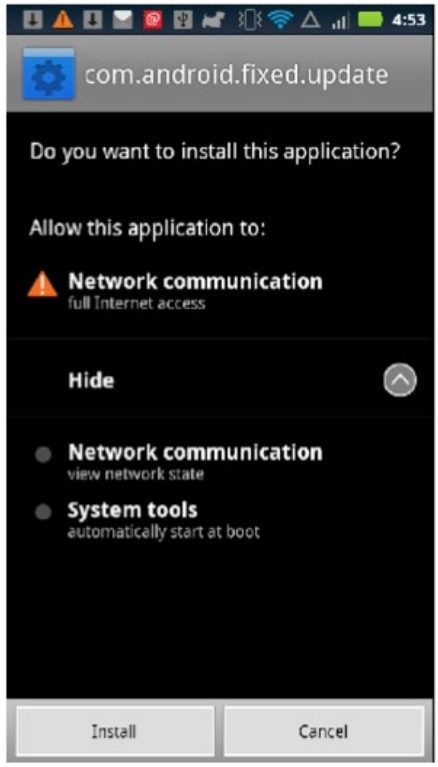
VirusTotal shows how this sample is named by the Anti Virus community. The name “NotCompatible” comes from an early version that used a ruse about the Android browser being not compatible with web site that served the malware. The malware was delivered as an update to fix that fictional problem. The “NioServ” names come from the fact that the malware used the Java NIO (New I/O) package for TCP/IP communication.

Data provided by VirusTotal ® on 2013-11-28.

Comodo	UnclassifiedMalware	**Sophos**	Andr/Notcom-A
Symantec	Android.Notcompatible	**Avast**	Android:NotCom-A [Trj]
DrWeb	Android.Proxy.1.origin	**VIPRE**	Trojan.AndroidOS.Generic.A
TrendMicro-HouseCall	TROJ_GEN.F47V0319	**AntiVir**	Android/Proxy.A
Kingsoft	Android.Troj.at_Nisev.a.(kcloud)	**NANO-Antivirus**	Trojan.Nisev.bkqvoh
F-Prot	AndroidOS/NotCom.A	**GData**	Android.Trojan.NioServ.A
ESET-NOD32	a variant of Android/NoComA.B	**BitDefender**	Android.Trojan.NioServ.A
Ikarus	Trojan.AndroidOS.NotCom	**Emsisoft**	Android.Trojan.NioServ.A (B)
Kaspersky	HEUR:Backdoor.AndroidOS.Nisev.b	**MicroWorld-eScan**	Android.Trojan.NioServ.A
F-Secure	Trojan:Android/NioServ.A	**CAT-QuickHeal**	Android.Nisev.B2983
ClamAV	Andr.Trojan.NotCompatible	**AVG**	Android/Nise
Baidu-International	Backdoor.AndroidOS.Nisev.AO	**McAfee-GW-Edition**	Artemis!0E8525862F9C
TrendMicro	ANDROIDOS_NISEV.VTD	**Fortinet**	Android/Compatible.A!tr.bdr
McAfee	Artemis!0E8525862F9C	**Commtouch**	AndroidOS/GenBl.0E852586!Olympus
Ad-Aware	Android.Trojan.NioServ.A	**Bkav**	MW.Clod0e8.Trojan.5258
K7AntiVirus	Trojan (0040f2631)	**K7GW**	Trojan (0040f2631)

INFECTION

Phishing spam is used to lure the victim to an infected web site, where an embedded <iframe> causes the browser to automatically download a file called update.apk. The user must then install it by clicking on the downloaded file and following the manual installation process.



Once installed, there is no application icon on the screen or any user interface to interact with. This is because the malware has installed itself as a background service that is only started when the screen is unlocked by the user or the device is re-booted. The malware service listens for the ON_BOOT or USER_PRESENT intents.

The only evidence that the malware is installed is through the “Manage Applications” section of “Settings”. This will show that an application called “com.android.fixed.update” is running. You can get rid of the infection by uninstalling the application.

OPERATION

When the malware service starts, it opens a configuration file called “data” in the res/raw directory. This is encrypted using AES and a password hard-coded in the code. The configuration file contains the address and port number of a primary and backup server to contact. The infected device opens up a TCP connection to the primary server. A fairly sophisticated command and control protocol is then used to multiplex TCP proxy services over that connection. These proxy services are predominantly used to access web sites from the infected device on behalf of the C&C server. Presumably the attacker is using this botnet to provide anonymous web browsing services to clients, but there are other potential uses.

```
class Config
{
  private String CIPHER = "AES/ECB/NoPadding";
  private String KEY_ALG = "AES";
  public Context Owner;
  public int Port1 = 0;
  public int Port2 = 0;
  public String Server1 = "";
  public String Server2 = "";
  byte[] key;
  int lastShow = 0;
  public String passkey = "ZTY4MGE5YQo";
```

The malware uses the Java NIO package to manage the TCP data communications with custom code to parse the C&C protocol and multiplex the proxy operations over the connection to the C&C server.

COMMAND AND CONTROL

An analysis of the network traffic shows a fairly sophisticated command and control protocol.

The command/response packets have the following format:

0x04	chan	type	length	…data…

0x04 - Protocol Version (1 byte)
chan - Multiplexor Channel number (2 bytes, little endian)
type - 0x00:Proxy Data, 0x01:Command (1 byte)
len - Length of the data field (4 bytes, little endian)
data - Is either proxy packet data or a command depending on “type”

The channel number is used to relate commands to responses and link proxy data blocks to specific proxy requests.

When commands are present in the data field, the first byte indicates the type of command. The following were observed.

```
Initial handshake:      | 00 | 07000v00 |
Proxy to IP:            | 01 | 00 | 4 byte IP | 2 byte port |
Proxy to domain name:   | 01 | 01 | LL | domain name | 2 byte port |
Response to proxy:      | 02 | nnnn |
End of proxy session:   | 03 |
Ping:                   | 04 |
Pong:                   | 05 |
Unknown (from victim):  | FC | 01 |
Set Timeout:            | FD | timeout |
Set Reserve Server:     | FE | server IP and port |
Set Primary Server:     | FF | server IP and port |
```

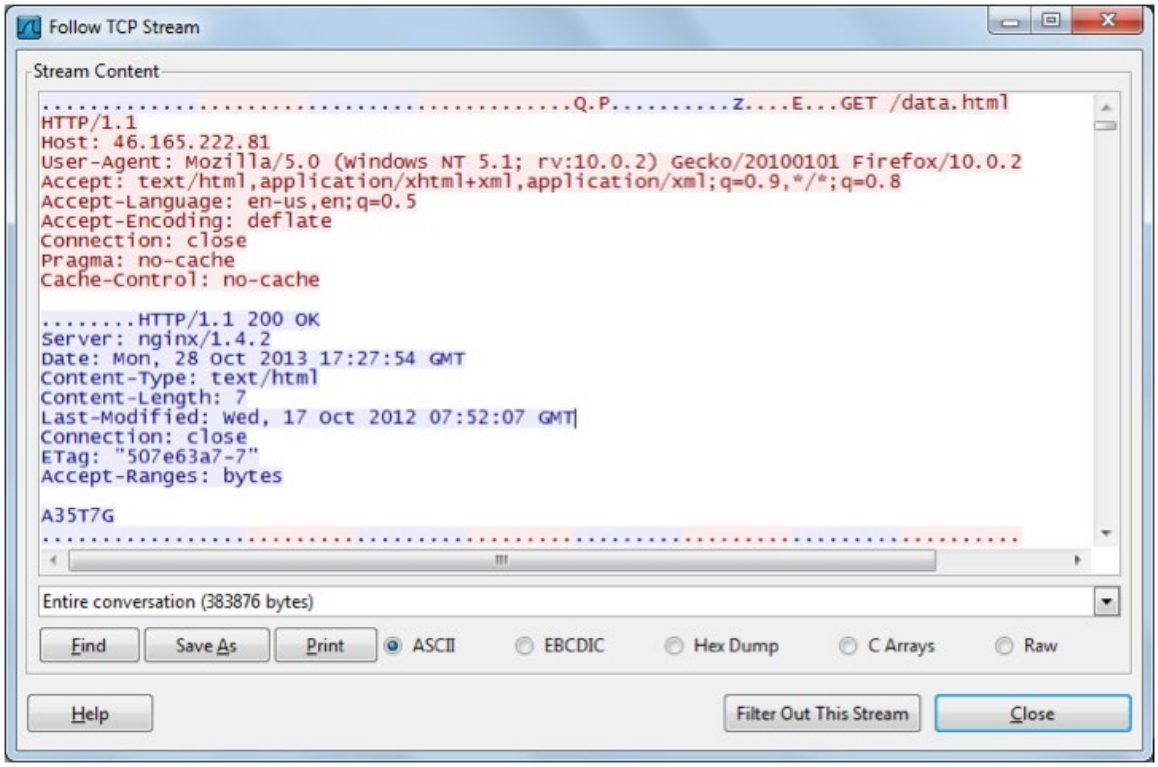
The ping and pong appear to be used as a heartbeat when there is no proxy work to be done. Once a proxy request is issued the “raw data” commands are used to transfer the data in either direction.

A typical proxy sequence would be:

```
C&C > Phone     | 04 0200 01 . . . . | 01 | … |     (request to proxy)
Phone > C&C     | 04 0200 01 . . . . | 02 | … |     (yes to proxy request)
C&C > Phone     | 04 0200 00 . . . . | . . data to send to remote site . . |
Phone > C&C     | 04 0200 00 . . . . | . . data returned from remote site . . |
C&C > Phone     | 04 0200 00 . . . . | . . more data to send . . |
Phone > C&C     | 04 0200 00 . . . . | . . more date returned from remote site . . |
Phone > C&C     | 04 0200 01 . . . . | 03 |          (end of proxy session)
```

Above we show only the packet header and the command byte, if present. In this case the channel number is 0x0200. Any data transferred (0x00) or commands (0x01) are associated with the initial proxy request on that channel. The last command terminates the transactions on that channel. Subsequent requests will increment the channel number.

The initial proxy request was very interesting and might be a mechanism for verifying the behavior of the proxy. The C&C server asked to proxy to retrieve the URL "/data.html" from a web server running on the C&C server itself. The proxy retrieved this URL and then echoed the response back to the C&C server. This response contains the string "A35T7G".



NETWORK IMPACT

When the requesting C&C server is active, the network impact of the proxy can be quite significant, but there were also times when activity was low for extended periods. More extensive test is required to measure the long term network impact of this infection, but the following cases were observed.

FIELD RESULTS FROM DETECTION SIGNATURE

The incident that triggered our interest in this malware in the first place was the high bandwidth usage from infected devices. In one instance an infected phone used 165 Mbytes of bandwidth in just under two hours. The vast majority of this was used by the malware to provide the proxy service. This could result in some very large data charges for the infected user, particularly if they are roaming. It would also significantly impact their battery life.

LAB RESULTS

The sample we used for this analysis was run in our lab for 6.5 minutes. During this time it transferred 1.57 Mbytes of data (~ 4 Kbytes/second). This is just under 100 M per hour, which is in line with the field result described above.

USES

There are a number of uses for this type of proxy service.

- Anonymous browsing services (probably the most common use case for this malware)
- Access to restricted foreign content
- Web Site optimization fraud
- AdClick fraud
- Internal network probe and data exfiltration (Enterprise APT case)

ANONYMOUS WEB BROWSING SERVICE

The most obvious use of this malware of to provide an anonymous web browsing service. People will pay for this type of service to conceal their browsing activities for a variety of reasons, particularly if the browsing activity is criminal in nature. User of the service would look like their web browsing is originating on the infected computers that are running the proxy service. So a person in Europe or China would look like they are browsing the Web from Canada or the United States.

PROVIDING ACCESS TO RESTRICTED FOREIGN CONTENT

Often content such as movies is restricted to distribution within a specific geographic region. For example in Canada we do not have access to the US version of Netflix. This proxy could be used to provide illegal access to this type of restricted foreign content, by making the user “look” like they are within the correct geographic zone.

WEB SITE OPTIMIZATION FRAUD

Web Site Optimization companies execute campaigns to increase the number of visitors their customers web sites and often target specific demographics and locations. It is feasible they could enlist the services of this proxy service to generate web visits that look like they are coming from the target locations.

AD-CLICK FRAUD

Ad-Click fraud detection mechanisms often use IP address geo-location to verify that the ad-clicks are coming from a reasonable location. For example it would be very suspicious if a lot of Russian IP addresses are clicking on Canadian advertisements. This type of proxy could be used to ensure that the fake ad-clicks are coming from a reasonable location.

APT PROBING AND EXFILTRATION

This type of proxy could be a key component in an “Advanced Persistent Threat” scenario. If a device inside a corporate network is infected, the attacker can use the proxy to connect to computers and services inside the corporate network and exfiltrate the data.

CONCLUSION

NotCompatible is noteworthy in a number of ways. It is the first Android malware we have seen to share a C&C infrastructure with a Windows bot, it has a fairly sophisticated C&C protocol, it is probably monetized by providing an anonymized web browsing service to the attacker's clients. In other words, it looks like a fairly mature Windows PC based malware application has been ported to the Android.

The malware is obviously making money since the spam campaign to distribute it is seen as a worthwhile expense.

The infection rate from the field shows that around 0.03% of mobile devices are infected. This may not seem like much, but the bandwidth consumption can add up. For example in a mobile network with 1 M devices, 300 will be infected and would consume a total of 720 GBytes of data per day.

The malware runs in the background as a service and its operation is not noticeable to the user. However it will likely consume considerable battery power when active, which will raise suspicions. In addition, users with a capped data plan will very quickly notice some very large charges on their bill. So it will be more difficult for this malware to remain unnoticed for extended periods, than it is for its Windows cousins. Most mobile anti-virus products will detect and remove the threat by uninstalling the app.

www.alcatel-lucent.com/solutions/kindsight-security

NP2014014010EN (January)

Alcatel·Lucent