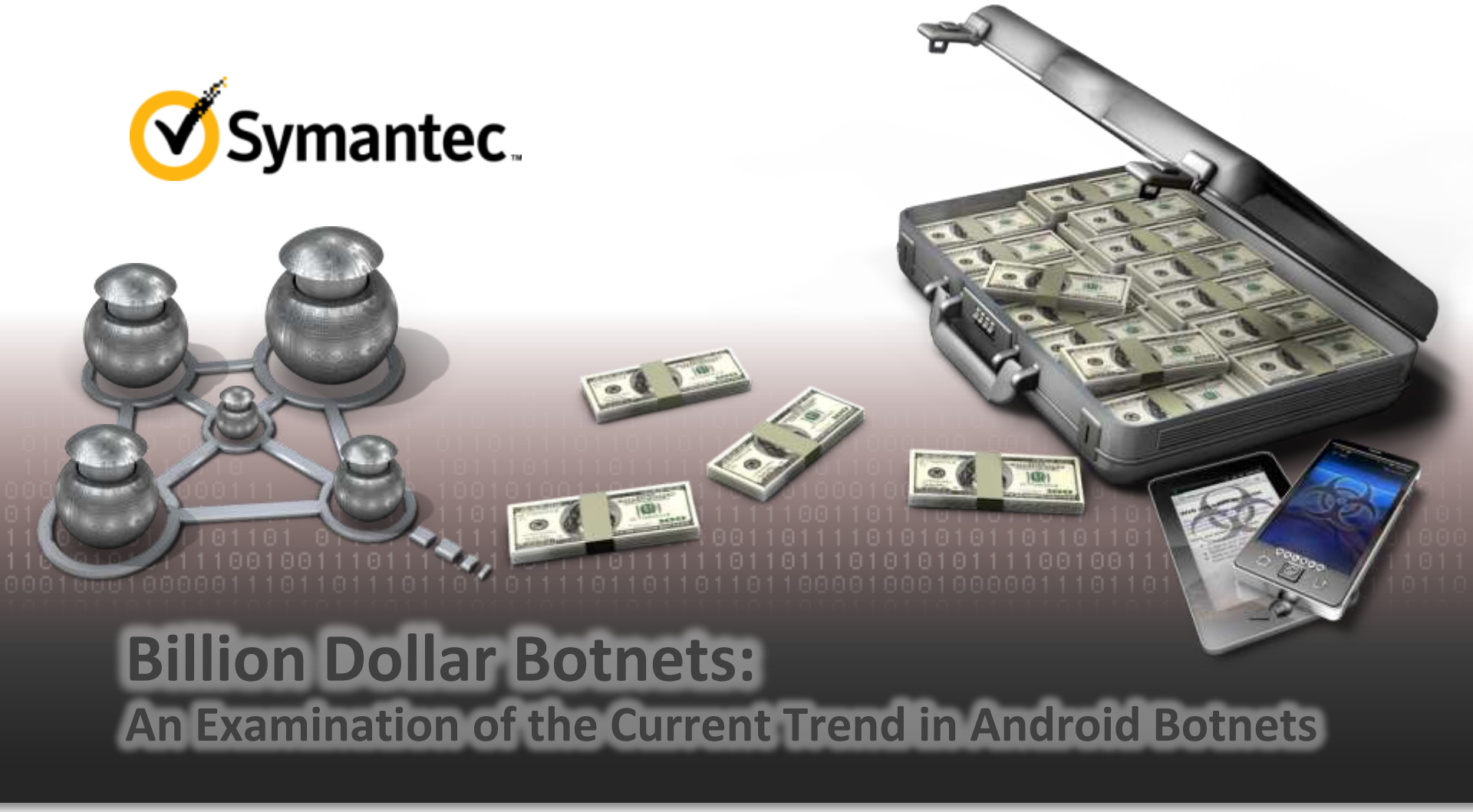
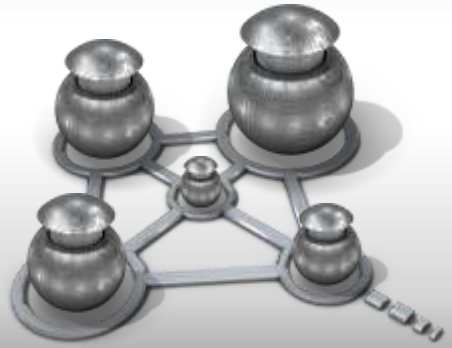


Billion Dollar Botnets:
An Examination of the Current Trend in Android Botnets

Cathal Mullaney
Senior Software Engineer
@threatintel

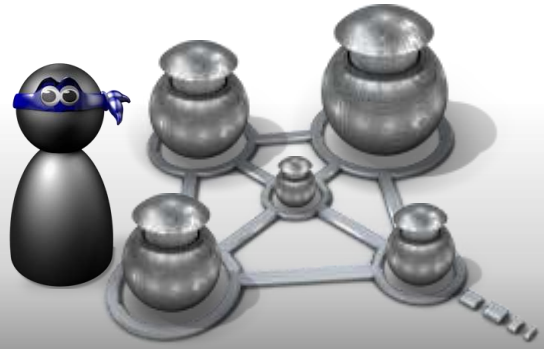
Presentation agenda

1



Android botnets overview

2



Bmaster botnet in-depth

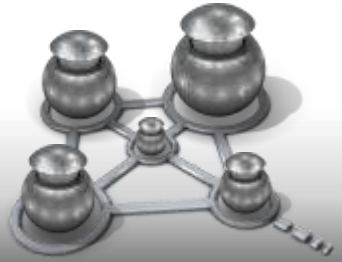
3

Bmaster revenue generation

4

Demonstration of C&C infrastructure

Introduction



- Android Botnets
  - Trending on devices now…

- MDK Botnet
  - 1 million active infections.

- Android.Bmaster
  - Botnet with a lot of telemetry!

Android Malware

Proliferation of smart phones.

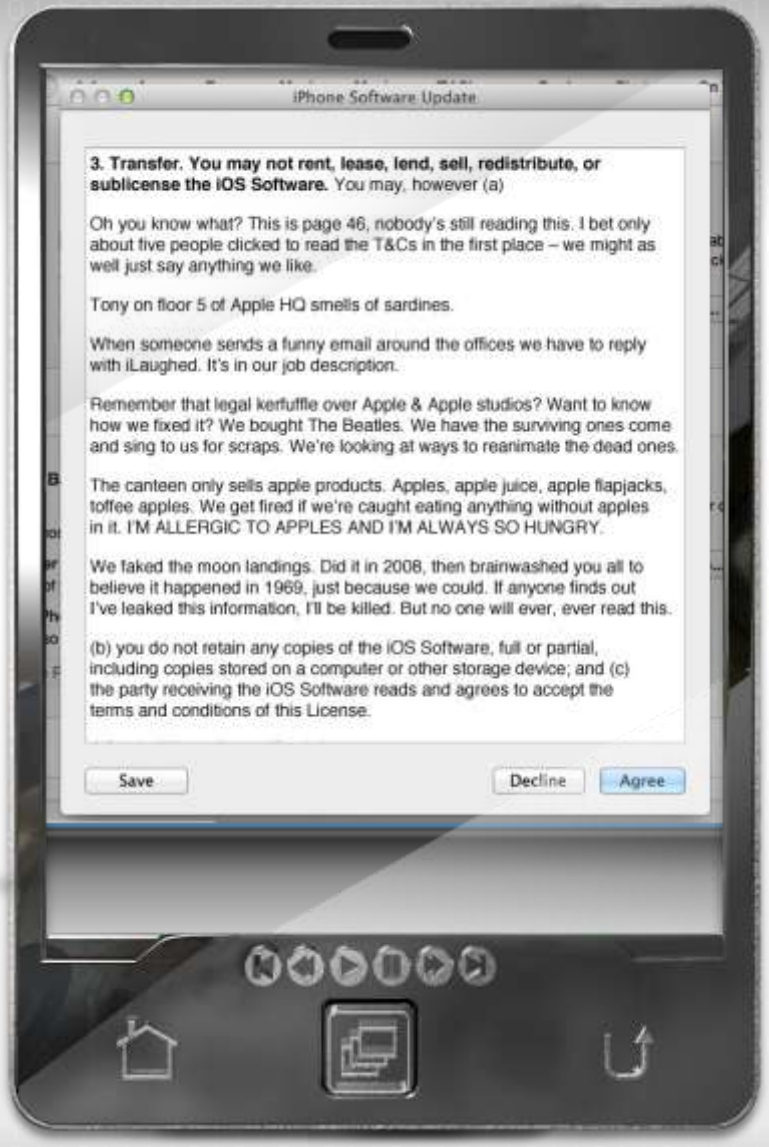
3rd Party markets with lax security.

Simple to write Trojanized applications.

Simple to write powerful malware.

Android program model suited to writing low profile Daemon processes.

Just install my malware already!



Screen capture taken from theHuffPost UK Comedy - http://www.huffingtonpost.co.uk

Android Malware

Simple to make revenue from infected devices.

Permissions are quickly becoming software EULA.

Charging for one or two transactions a day may not be noticed immediately.

Mobile banking applications are on the increase.

*Looking at you Hesperbot!

Android.Bmaster

Ghost in the (mobile) machine.

@threatintel

Infection Vector

2 Trojanised APK downloaded to victim's phone.

1 Smartphone user contacts app store.

Infection

4 C&C sends Exploit/RAT

3 Trojanised APK registers with C&C.

Infection Vector

Hosted/Spammed on 3rd party, Chinese, Android market place

Legitimate software trojanized with the malware.

Infected 3rd party software

Trojanized applications are a common infection vector

Trojanized application was a loader/downloader for the larger botnet/exploit program.

Seems legit...

But actually...

Bmaster Loader

1. Registers with C&C
2. Exploits Device
3. Installs Malware
4. Tracks Phone
5. Charges user

Malware operation

1. After decryption malware contacts the remote URL, downloads and executes the GingerBreak exploit.

2. Exploit may fail, but regardless the malware will then attempt to download a RAT (Remote Administration Tool).

3. RAT registers with CnC, Depending on configuration Assigned to a “channel”.

4. Main functionality is for revenue generation.

Return of the RAT

- Registered three main services and several intent filters/broadcast receivers.
- Services used to generate revenue for the Botmaster.
  - Send an SMS to a number.
  - Connect to a URL.
  - Connect to an IVR.
  - Poll the C&C for new commands.
- Intent filters to capture/block SMS messages received, outgoing calls made and boot of the compromised device.
  - Among many others.

Malware operation

3 Infected device is charged and attacker gets paid.

1 C&C Issues command to device.

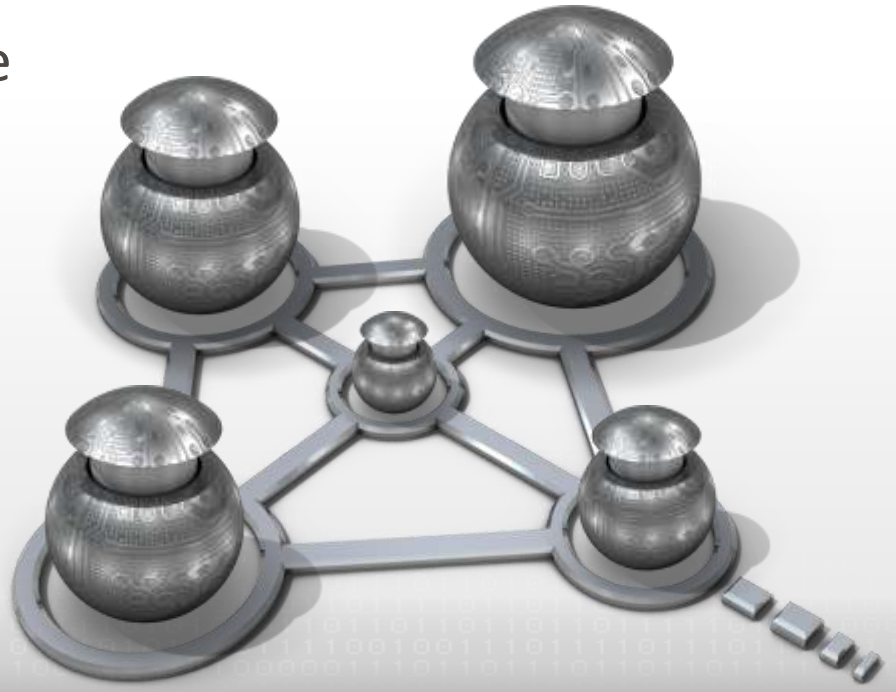
2 Device contacts premium services

C&C Server

- Communication between device and server using KSOAP.
- Poorly secured servers.
- Server contained a complete C&C infrastructure interface.
  - Maintained data on infected devices.
  - Infection rates.
  - Successful Revenue generation.
- A complete picture of the Botnet and potential revenue generation emerged.

Android Botnet

- Judging by available timestamps we estimated the Botnet operating from September 2011 to present?
  - C&C infrastructure went dark.
- Infected devices numbered in the hundreds of thousands.
- All devices that were capable of revenue generation were stored for potential activation.
  - Sleeper cell phones.



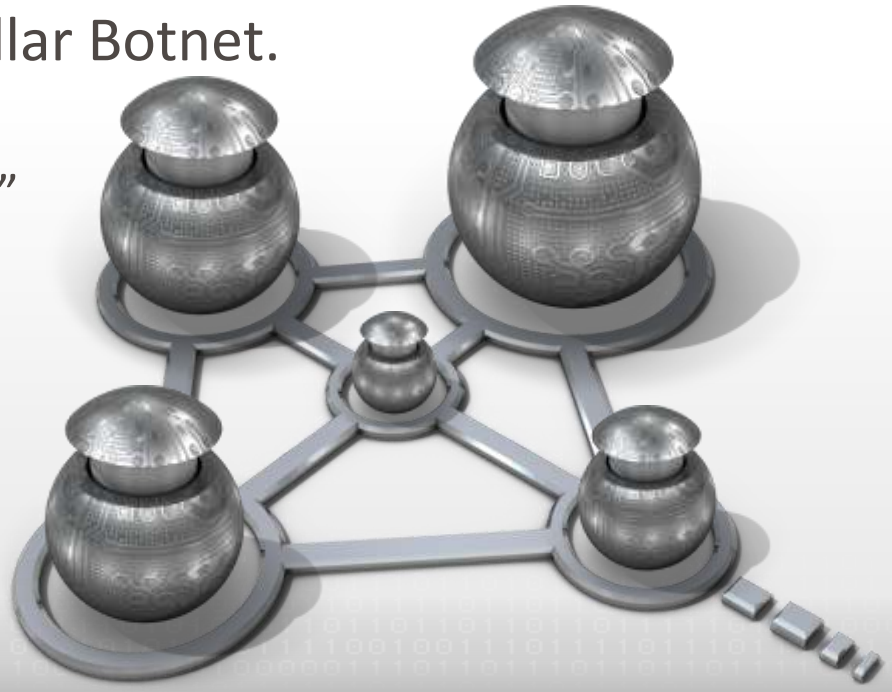
Revenue Generation

- All infected devices broken up into channels.
- Channels allowed the Botnet master to control huge amounts of devices by issuing a few commands.
- Revenue is generated by sending SMS to premium numbers, contacting PPV websites and premium telephony services (voice chat lines).
- The Botnet master can also configure how many times per day these services are contacted (default to three).

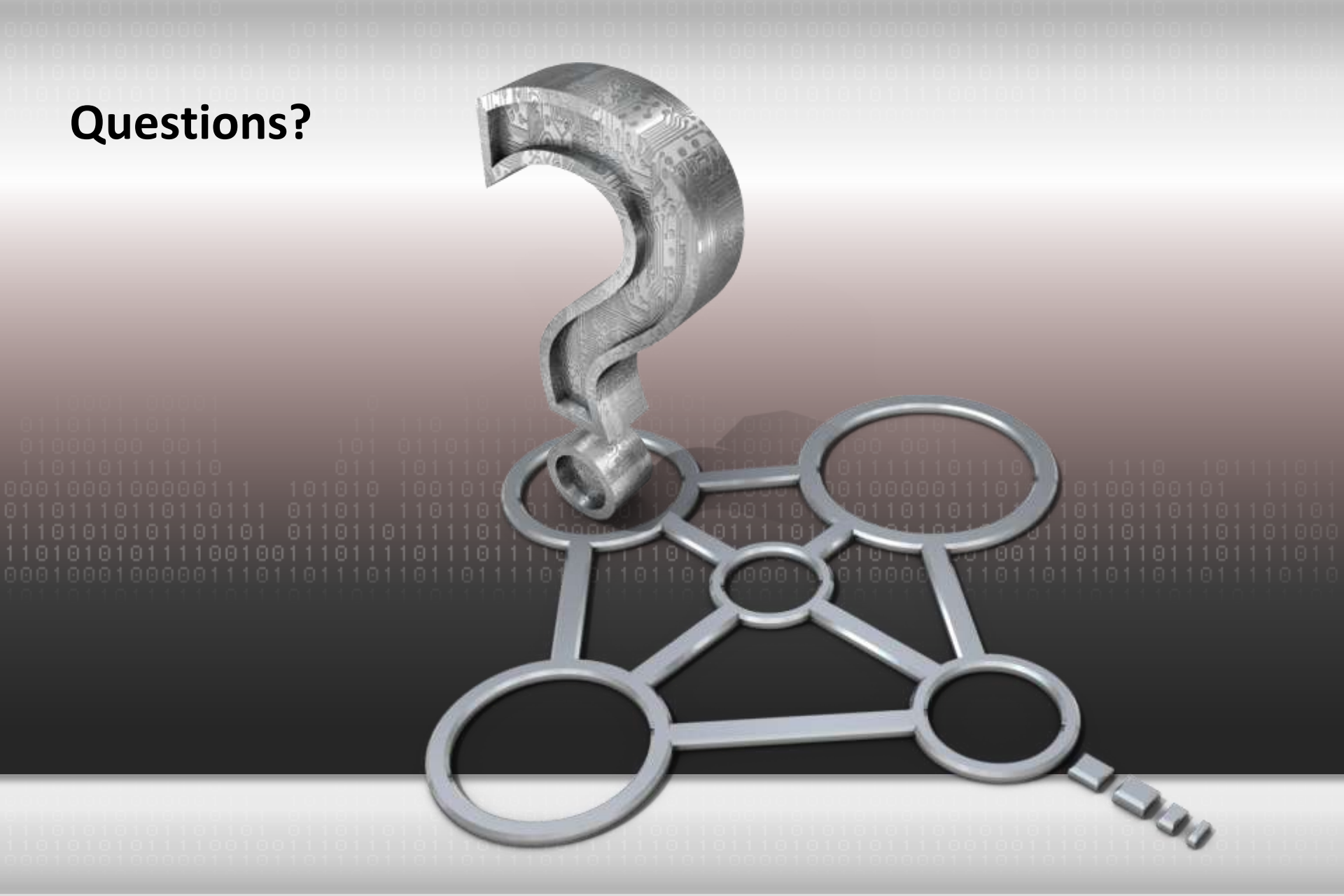
Botnet management interface demonstration.

Conclusions

- Android malware is simple to disseminate to a wide user base.
- Huge new markets for Malware writers emerging.
- Potential revenue in the millions of dollars.
- Entering the age of the billion dollar Botnet.
  - Real question is: “Why wouldn’t malware writers target aggressively?”



Questions?



Thank you!