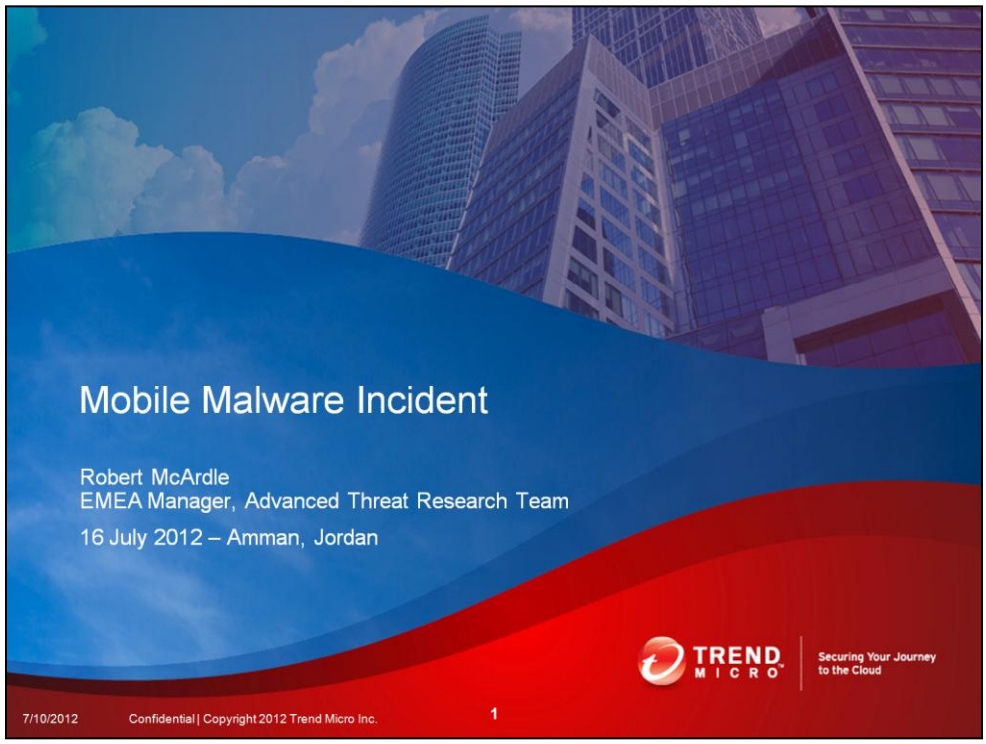
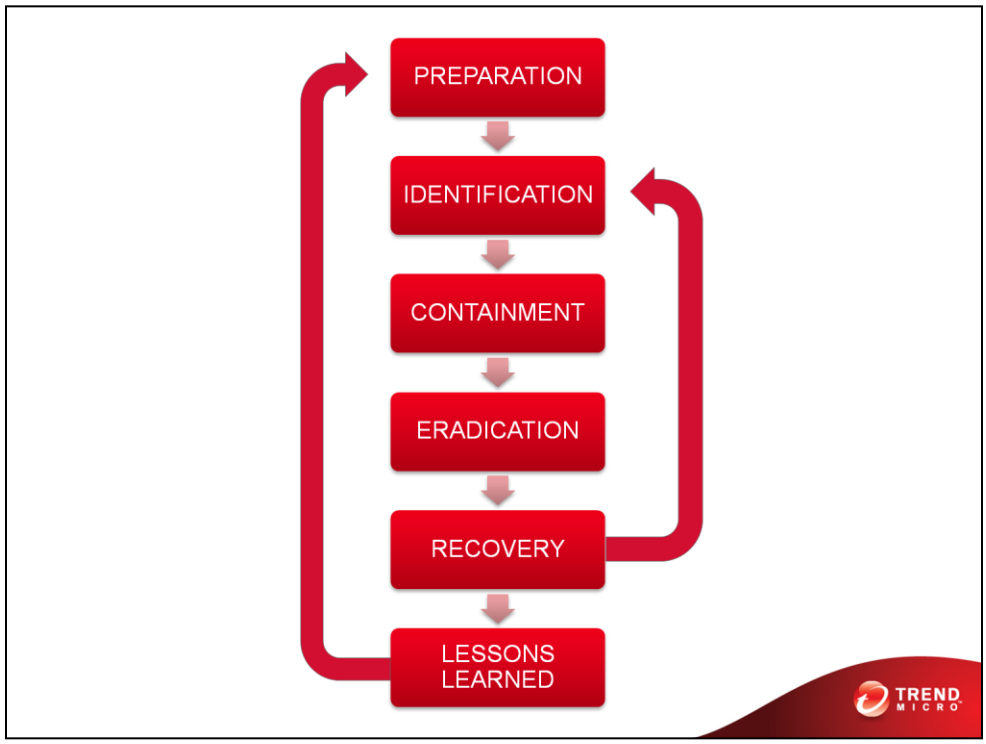


For this part of the workshop we will take an example mobile malware incident, and then you can break into groups and see how you would respond to it.

At the end of this session I'll step through some hints on how to handle such an incident in the future

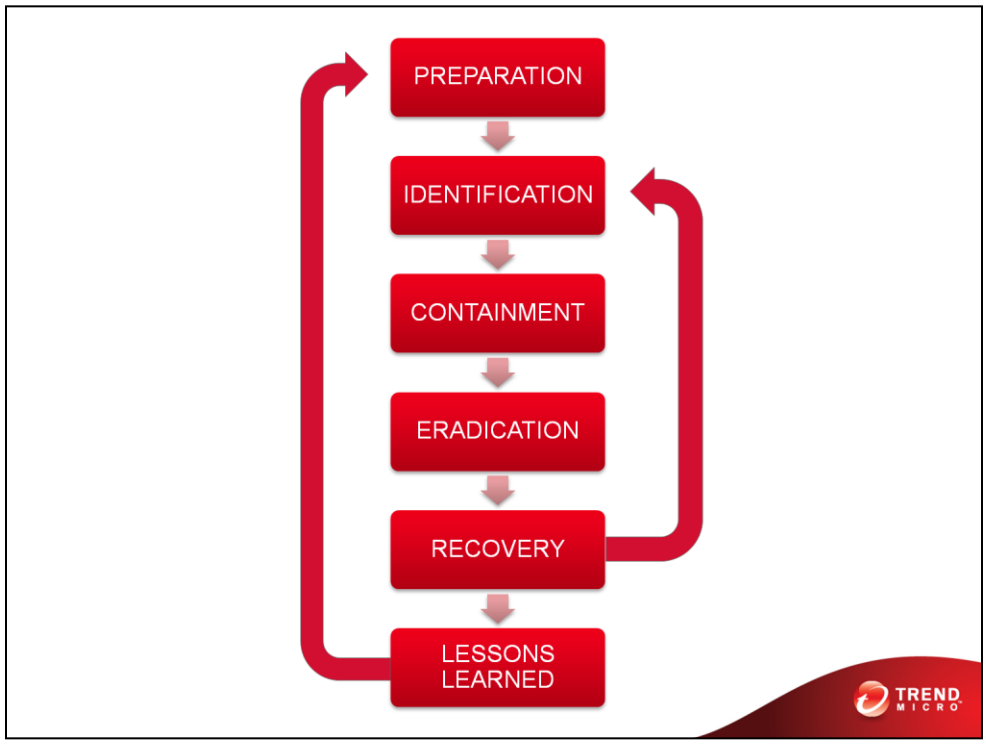


Lets start with a very short overview of an Incident Handling process – I assume everyone here is at least somewhat familiar with the normal stages of handling an Incident – but just in case, heres a recap

Firstly what do I mean by an Incident. I mean “an event, or series of potentially malicious and unusual events on a computer network”. There are two key events here – the events have to be different from normal behaviour in the network AND they need to imply a level of harm. Take this example – imagine you see a number of failed logins from several employees all in the space of 5 minutes. That could be an incident. However if it is the first day back after 2 weeks of Christmas holidays, this could be normal (people forgetting logins)

There are 6 stages in the classic incident handling model. The first is preparation, this is everything you do before an incident occurs – and is what occupies most of your time. Making contacts, policies and procedures, buying hardware etc – all of that is part of the preparation stage.

Next comes identification – this is were we decide is something is an simply an event, or declare an incident. This is where detection takes place for example in a mobile malware incident



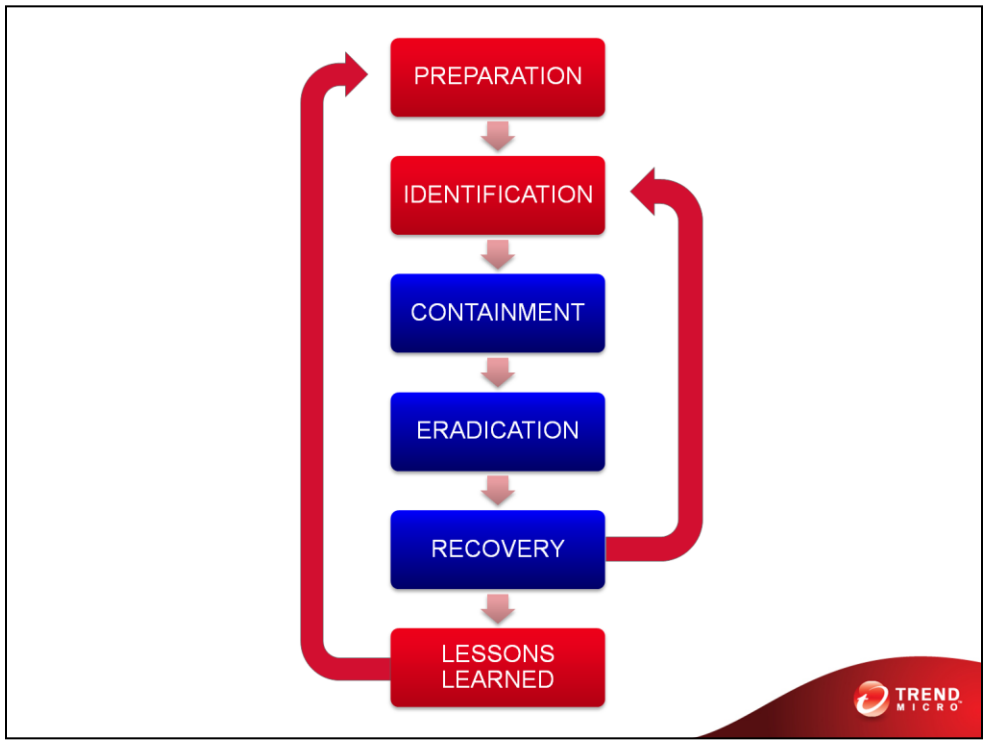
Next we have containment. Simply put this is about “stopping the bleeding”. The goal here is not to clean up the incident – but simply to stop it getting any worse

After that we have Eradication – removing all traces of an attack, and getting things back to normal.

Putting any system we have taken offline (normally during the containment phase), back online – all of that occurs during the recovery phase. It is also really important in this phase to monitor any systems involved in the incident, as attackers will regularly come back

And finally we have Lessons Learned – the part most people forget to do. It is really important to document and compile a report of everything that happened during an incident as soon as possible after the incident has been resolved. Most people are already tired at this point, but this is the time when all of the details are fresh in your memory. The recommendations from this phase feed back into the Preparation stage – so that the whole process is a cycle.

In fact there is another cycle in here too – often you will think you have removed all parts of a threat, and put affected systems back into production – only to discover that the attack is still ongoing. This is normally a sign that you missed something during the identification phase, and need to go back and do more analysis.



In the exercise we are going to do today we will concentrate on the Containment, Eradication and Recovery phases. You will be given the information that has already been gathered during the Identification phase.

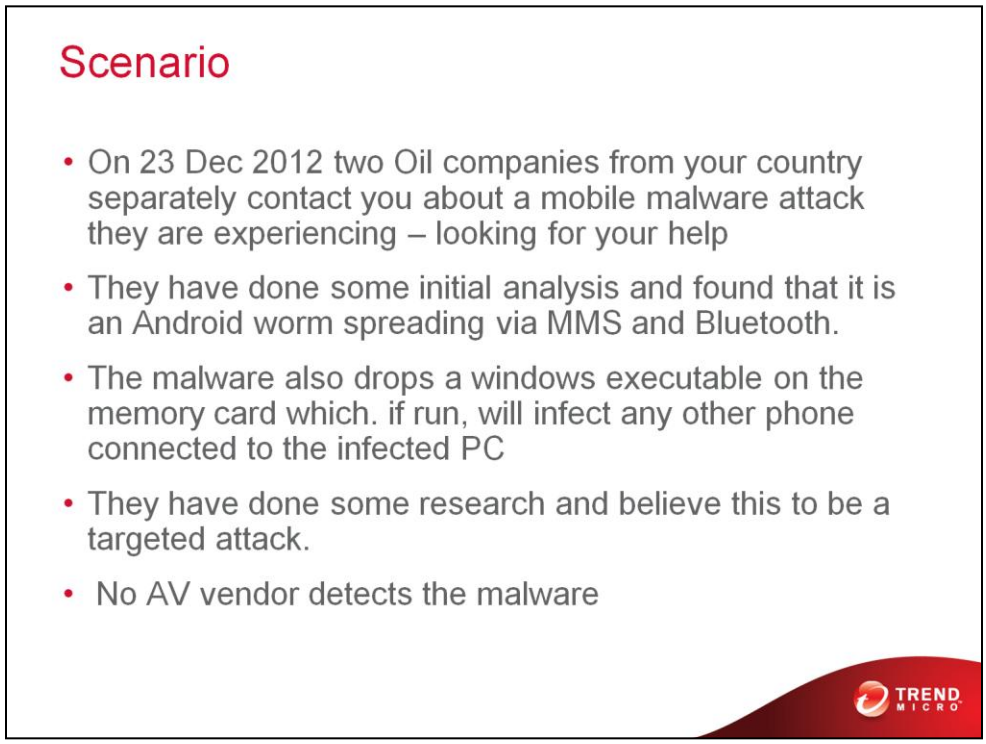
So the plan for this session is that I will read through the example scenario, and also hand each group out a copy.

Each group then has 25 minutes to discuss the incident and write down recommendations for what a CERT could do during such an incident – focusing on the three stages of Containment, Eradication and Recovery. So that's "Stopping things getting worse", "Cleaning things up", and "Putting things back to normal and monitoring"

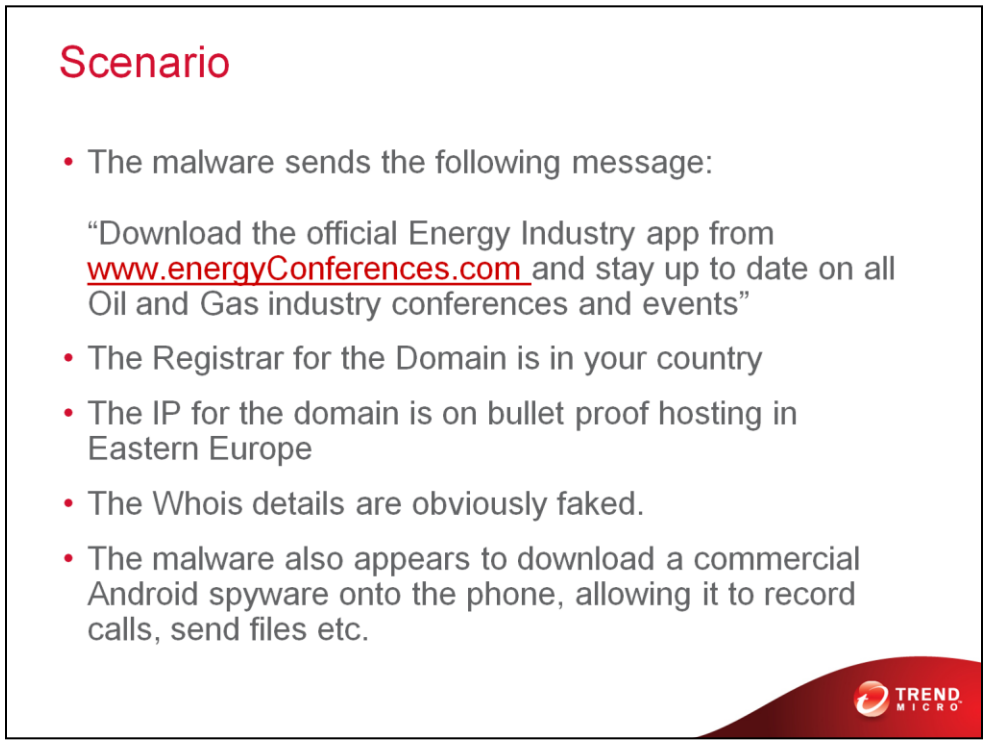
At the end of those 25 minutes – I'll run through some recommendations of my own for how to handle a mobile malware related incident. I'll then ask everyone if you came up with any suggestions I had not covered, and that way everyone can learn from each other.

The goal here is of course to get you thinking about how you would handle a mobile malware incident. Of course 25 minutes is a short amount of time, in reality incidents last hours or days – but at least it's a good start.

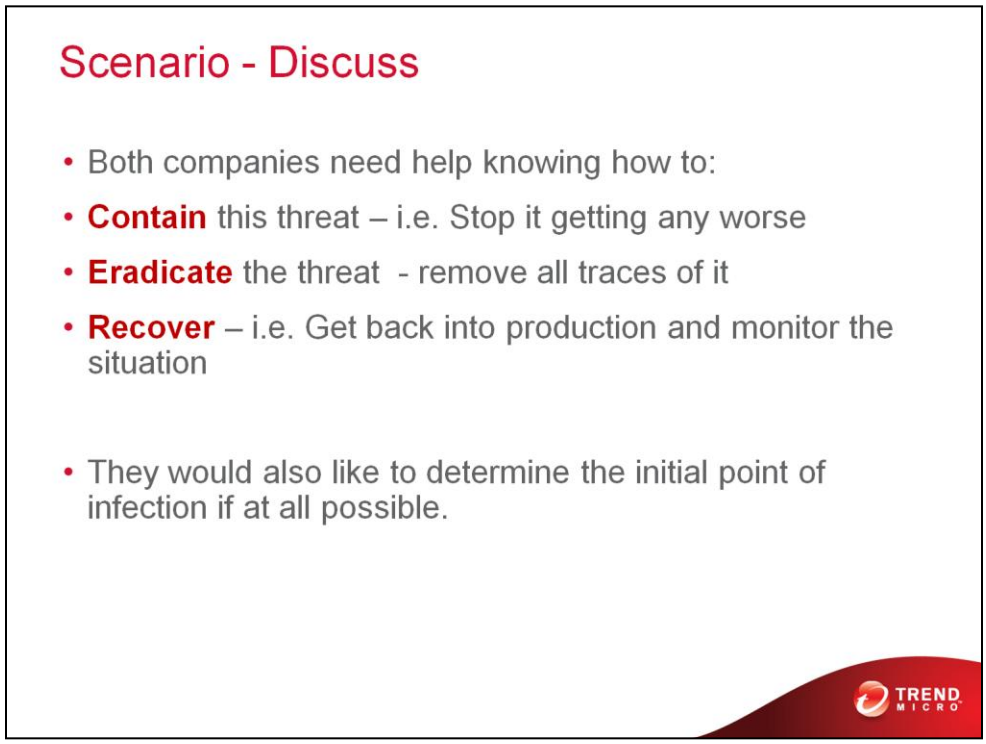
Ok? Any questions?


Scenario
• On 23 Dec 2012 two Oil companies from your country separately contact you about a mobile malware attack they are experiencing – looking for your help
• They have done some initial analysis and found that it is an Android worm spreading via MMS and Bluetooth.
• The malware also drops a windows executable on the memory card which. if run, will infect any other phone connected to the infected PC
• They have done some research and believe this to be a targeted attack.
• No AV vendor detects the malware
TREND MICRO

SCENARIO

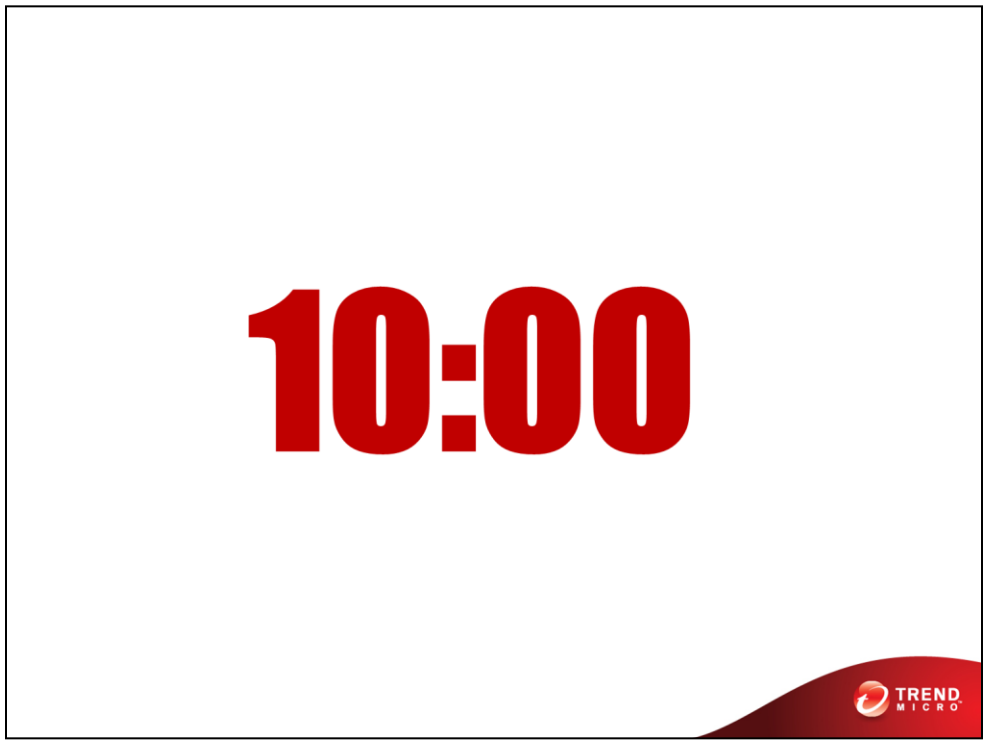

Scenario
• The malware sends the following message:
"Download the official Energy Industry app from www.energyConferences.com and stay up to date on all Oil and Gas industry conferences and events"
• The Registrar for the Domain is in your country
• The IP for the domain is on bullet proof hosting in Eastern Europe
• The Whois details are obviously faked.
• The malware also appears to download a commercial Android spyware onto the phone, allowing it to record calls, send files etc.
TREND MICRO

SCENARIO



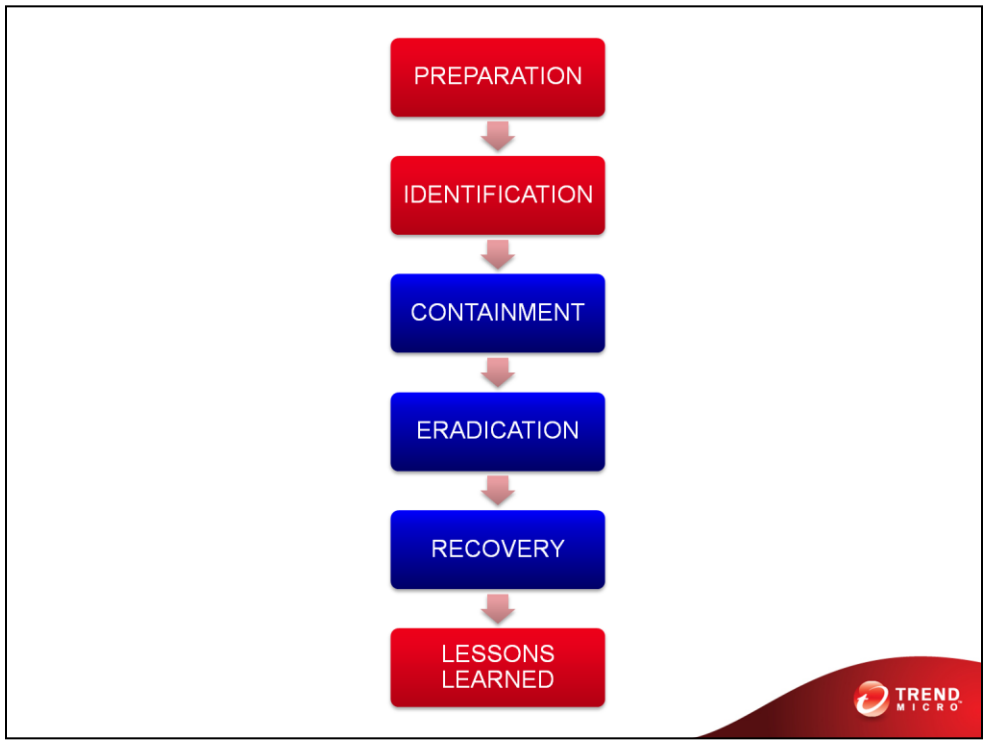
SCENARIO

25 mins left



10 mins left

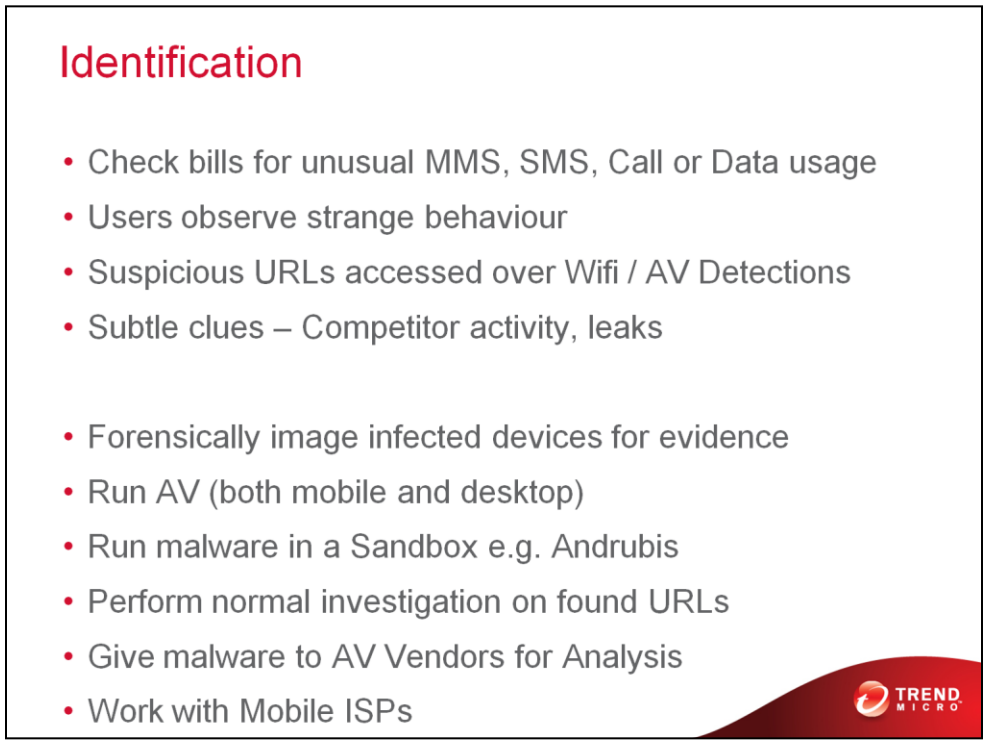
5 mins left



Ok then – to recap. I asked you to have a look at a mobile malware scenario and come up with a list of recommendations for the Containment, Eradication and Recovery phases.

I'm now going to step through each phase and give some personal recommendations – and then we'll start a discussion.

In my case I'll actually start with the Identification phase. It was not covered in this incident, but its useful to go through so you are aware about if for any incidents you may phase yourself. I'm leaving the preparation phase alone for now because pretty much all of the recommendations we come up with will feed into that stage in some way.



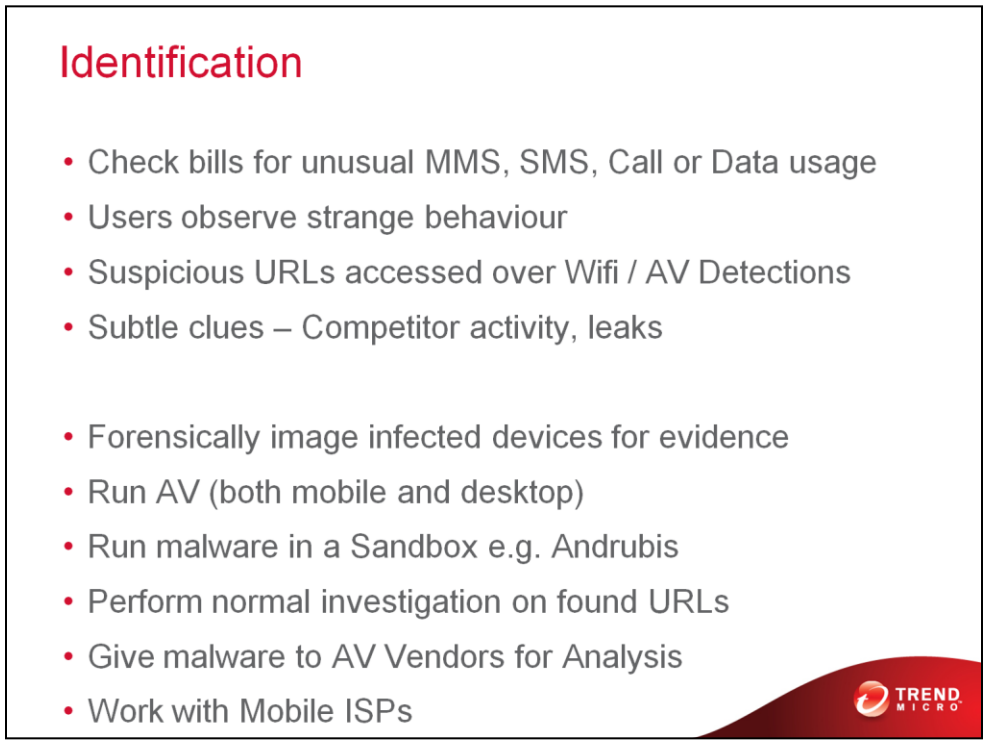
Sometimes on of the earliest signs of a mobile infection will be discovered by monitoring a companies bills. Two things are very important here – first to know what "normal" phone usage looks like, and secondly to have the ability to check these logs on a daily basis (most mobile ISPs provide this via a web console).

Another early warning sign is users. They are the people who use their phones every day, so are the most likely to discover something wrong. That can range from shortened battery life (e.g. due to a Bluetooth worm), or contacts receiving unexpected messages from them

Another warning sign can be malicious URLS accessed via the phones while on the office Wifi environment. You normally will have no visibility over the 3G communications of the device, but while it is using the wifi for internet it can give some valuable clues. Obviously AV detections on the devices is also a sign of an incident. Enterprise mobile AV products will normally also have web blocking built in, in which case you can intercept malicious 3G traffic.

Lastly, a more subtle clue there is an incident can be seen in competitor behaviour. If they look like they are acting on information they should not have access to for example. Or if some of your documents and information show up on the web or on sites such as pastebin. For Pastebin there are several monitoring tools available on the web.

So what should you do if you find a mobile malware incident?



There are numerous ways to forensically Mobile phones, with different models and different OS requiring different approaches. There are several guides online discussing these. It is important that you have several images of the phones backed up so you do not destroy the evidence during your investigation.

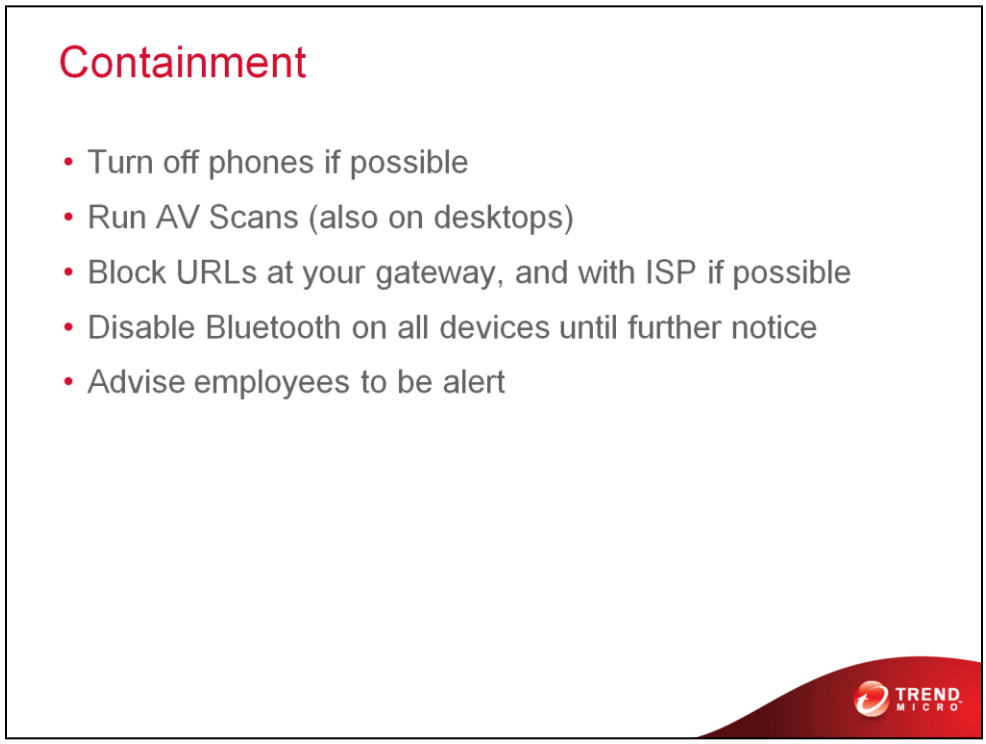
Next scan the infected device with AV – both a mobile AV, and use a desktop AV to scan a copy of your forensic image (but not the master copy).

For any found malware, you can run it in a sandboxed environment. You can either build one yourself – or use an online tool like Andrubis which is built using a variety of open tools such as Droidbox, TaintDroid, apktool and Androguard (http://anubis.iseclab.org/)

For any found URLS, perform your normal investigations (e.g hosting, registrar etc)

If the malware is undetected it is a good idea to send to AV vendors looking for a more indepth analysis. This is where establishing a good relationship with several vendors during your preparation phase is really useful.

Lastly having good contacts with the mobile ISPs in your country is extremely important. Its possible they can look to see who the first person to send a certain MMS, or access a certain URL was – giving an idea of the initial infection vector. This is especially important in high profile targeted attacks.



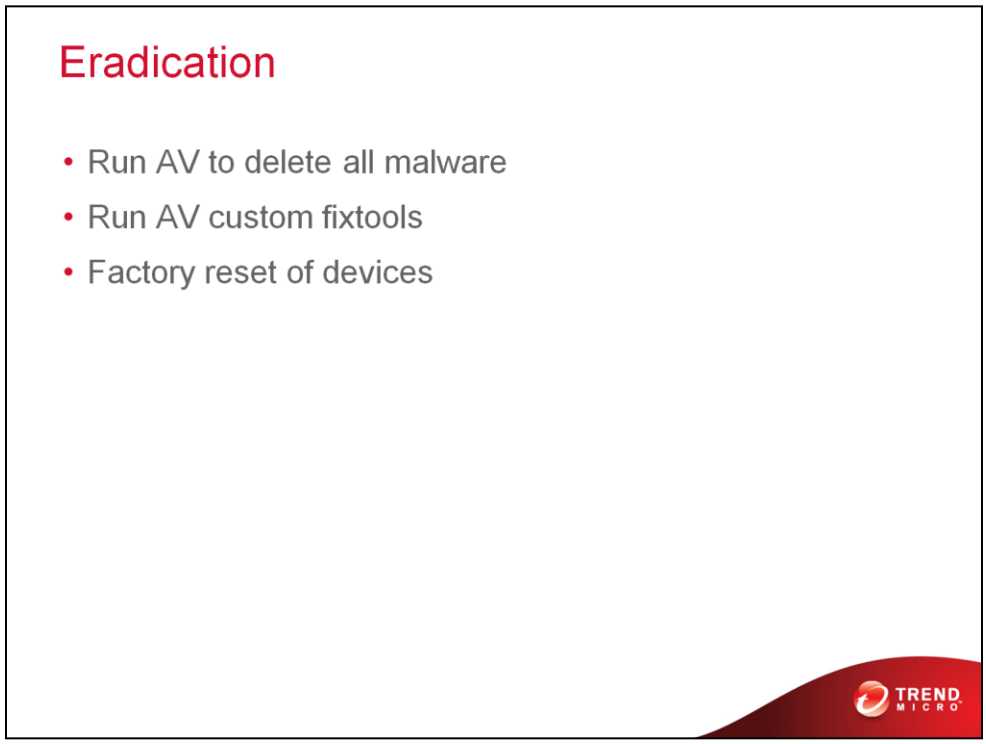
Next comes containment – stopping things getting any worse

Firstly try and turn off all phones affected if possible. This can be more difficult than it sounds. Does the company have a policy that allows them to order employees to temporarily deactivate their phones? What about the CEOs phone? What about people who use personal phones for work purposes? Also do you have a policy and procedures on being ably to securely wipe phones? Ideally those are not decisions you want to be making in the middle of an incident – but rather that you have discussed them at length during the preparation phase.

Next, and especially once AV vendors have updated their patterns, run a scan on all mobiles on the network. Also run a full scan of the desktop environment as the mobile incident may only be part of a bigger problem

You can also block all URLs involved in the attack at the gateway, and on your phones if your mobile AV supports that. If not you will need your mobile ISPs help – which is why such a relationship is really important. If you have a very good relationship with the mobile ISP they may even help you to sinkhole the domain – redirecting all traffic from that ISPs customers to a server under your control. The laws on this differ from country to country, and you may also see infected organisations outside of the original victim

Alerting employees can be very useful, especially if the organisation has been doing a good job with security awareness training. Employees are often one of the biggest security issues in an organisation, but they can also be turned into one of the best detections methods you have at your disposal.



Once you have stopped the problem getting any worse, the next step is to eradicate the threat

Once AV scanners have been updated, running a scan will often clear all traces of the mobile malware. Most mobile malware is not as complex as its desktop cousins – you are unlikely to see things like kernel level rootkits for example. In more extreme cases AV vendors can create custom “fixtools” to remove all malware traces

If possible factory reset all affected mobile devices. Here again policy is very important – are you allowed to do this? What data will be lost. Both Android and iOS provide several services that can actually make recovering the system pretty straightforward. iOS lets you backup all your apps, contacts, pictures etc to iCloud. Android can backup using Google contacts and Google Drive. Whether Google Drive and iCloud are allowed on a company network also needs to be discussed during the preparation phase.

Finally we need to get everything back into production, and monitor for any new attacks

First we bring any affected devices back onto the network. If any new software (e.g. mobile firewalls, remote wipe ability) need to be installed, it should be installed and tested before this phase

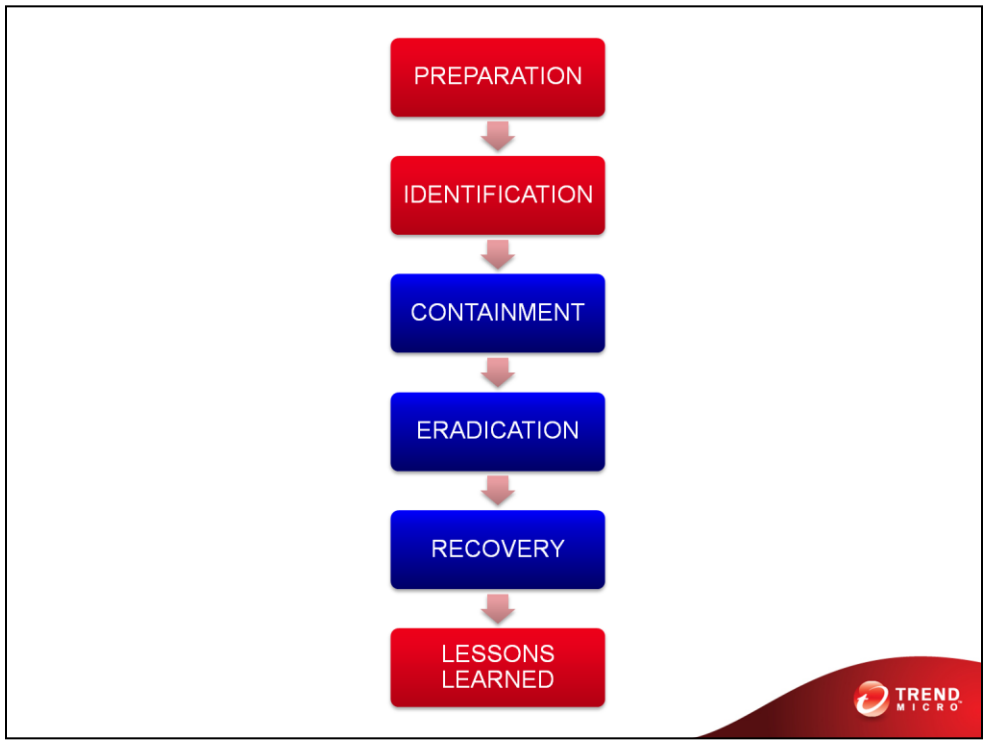
Observe the affected phones carefully. Do daily checks using billing on their data, message and call usage. Also take several phones back at random after several hours / days for inspection

Place the company help desk on high alert, and inform employees about the incident and to be on the lookout for more incidents

Finally work with mobile ISPs to look for ongoing signs of attack or new attacks, and monitor the web for leaked company data.

In the last stage of the incident handling process it is really important to create a thorough report detailing what occurred during in the incident, and recommendations to prevent such incidents in the future.

Some recommendations may include those on the slide. Especially for a CERT acting as the point of contact for AV vendors and ISPs can be really important.



DISCUSSION

So those are some of the recommendations I would personally give – but lets now open this for discussion on some of the suggestions your groups came up with.