SIX PUMP COURT

STEALTH OR SPOOF PHONES USED BY GANGS – A NOTE

RICHARD BARRACLOUGH QC, SIX PUMP COURT

DENISE BREEN LAWTON

AUGUST 2019.

INTRODUCTION

1. This note is based on the report and evidence of an expert ANGUS MARSHALL a forensic computing consultant given in a recent murder trial in Leeds Crown Court and his and PETER MILLER'S paper "Case Note: Mobile phone call data obfuscation and techniques for call correlation".

2. In 2017 law enforcement agencies investigating gangs saw that the usual techniques used to map contact between gangs based on call data records were not working properly. The investigators found that CDR (call data records) directed the investigators to unconnected innocent numbers or nonsensical unissued numbers.

THE ESSENCE OF THE SPOOF PHONE

3. A particular SIM (subscriber identity module) (a smart card used to allow mobile phones to operate on networks) marketed for legitimate purposes by one company permits the user to *"get off the grid….. It can hide its real number making it impossible to trace. You can even redirect all calls from multiple AY SIM cards to a single one for maximum protection*".

4. Such SIMs are designed to mask the number associated with the SIM so as to allow the SIM user to change the number presented to those he/she is calling at will and to allow others to call the handset in which the SIM is installed by calling one of several "*access numbers*".

   The technology results in false or difficult to trace numbers being recorded on hand sets and in call records.

5. A stealth SIM can be used to access the mobile phone network but makes use of a network of management features (USSD for user interaction/control and CAMEL for routing and handling) to mask its location and true identity from anyone receiving calls from it.

6. Stealth SIMs can be used to allow calls to be made to false numbers (either full numbers or short codes) in order to hide the identity of the called party.

7. USSD or unstructured supplementary service data is a data transmission and receipt service offered by GSM networks. It is usually used to communicate with network to retrieve account data. USSD messages handled by the home network normally start with an asterisk and are terminated with a hash.

   CAMEL or customised applications for mobile networks enhanced logic, permit SIM home networks to manage calls and cost. Because CAMEL interactions happen between networks it is rare that they are recorded in customer call data records or made available through billing data.

8. CAMEL functions permit the handset to be registered with a company automated switchboard so that calls made to an extension within the company can be automatically routed to the mobile handset and calls made from a mobile handset to be sent via the company switchboard. The direct dial number for the handset would not be apparent to callers or called parties. The switchboard can present any number as the CLID (calling line identity) when a call is routed through it. This method is used by cold callers and scam callers.

THE MECHANICS OF THE OPERATION

9. The SIM provider must be able to route calls via their own switchboard or a rented virtual switchboard. Such systems routing calls can be programmed by remote administrators.

10. Some providers offer stealth SIM or anonymous SIMs which permit users to appear to be located in other parts of the world, present falsified or spoofed CLIDs, prevent cell site geolocation and change the callers voice. The CLID is the calling line identity- the phone number disclosed as the calling number to handset which is receiving call. This is not necessarily the real number of the calling party as it can be changed using appropriate network technology (eg private switchboard systems)

11. Thus investigators may be prevented from obtaining data about locations and calls.

12. In the normal case the two handsets are registered with the mobile network via a cell site mast which has a unique identifier and the handset is identified by its IMEI and the IMSI of the SIM in it.

13. Stealth SIMs use network features which allow redirection to an alternative provider or route. The providers create their own Mobile Virtual Network Operators. They use SIMs from legitimate providers which are programmed to use such MVNOs as the home network.

14. The visitor location register is a register of IMSIs which have been authorised via their HLR (home location register) (a data base of active IMSIs which are authorised to use the network). The SIM which is roaming interacts with the HLR to check authorisation. The HLR via the CAMEL system returns a redirect request and the roaming network passes to an alternative number. The call is then handed over to a VOIP (voice over internet protocol) (a mechanism which allows calls to be carried over the internet).

The outbound VOIP gateway is programmed to send a false line identifier or CLID which can be changed to prevent patterns of calls.

15. Where the called and false incoming CLID appear to be mobile numbers no IMSI/IMEI or cell data for those numbers are available in the CDRs for the caller or the recipient.

INVESTIGATION INTO SPOOF PHONES

16. It is possible through the use of time based correlation technique, to corroborate the calls said to have occurred between identified parties, but this requires access to data from all the mobile networks which the SIM has used during the period of interest and requires data from the calling and receiving accounts.

17. Where only one handset is recovered or call data obtained from one side of the conversation it is not possible to determine who or where the other party was.

18. Where billing data for both caller and recipient are obtained, by examining start date and time, end date and time, type, calling number and called number a pattern may be detected. Start times may be several seconds apart depending on the mechanism (2 seconds for redirection and up to 15 seconds for call back). Where SIMs are configured to allow roaming across multiple networks it may be necessary to obtain billing data from several network providers in order to establish a complete pattern of activity.

19. If handset call logs are available, the presence of 0 duration outgoing calls immediately followed by incoming calls might suggest the use of the call back system

    Where a stealth SIM is in use, the called number recorded may not match the number dialled by the user due to the redirection mechanism.

    Thus one checks the end times of both calls on the two accounts believed to have communicated with one another and the call durations (to within 1 or 2 seconds) and where there is a pattern of such calls, it is reasonable to infer that the two accounts may be used by the redirection system to communicate with each other.

    If the calling number associated with the incoming calls is obviously false or a "*lazy*" number or a number used by an innocent third party) this implies that the number is spoofed.