(S//SI) A New Source of SIGINT: Exploiting Video from 3G Phones

FROM: Dan Aldridge and [redacted],
and SIGINT Communications
Run Date: 02/15/2006

(S//SI) Cell phones with video capability may have started out as a mildly exotic technology, but they are rapidly becoming the norm! In fact, the day may not be far off when it will be impossible to buy a cell phone that does ***not*** come equipped with a built-in camera as a standard feature. NSA's targets have found such camera phones useful for a variety of purposes and regularly send video footage to each other from even the most remote corners of the globe. Given this potentially lucrative source of SIGINT information, efforts are underway in SID to find the best ways to exploit these signals.

(U) The VCR Pod

(S//SI) The Video Communications Research Pod (Pod 40) studies image communications, both still and moving images, with a current focus on camera cell phone videos and video attachments to email. Early efforts by VCR Pod members have produced fascinating results with regard to 3G camera cell phone video exploitation. Pod members are investigating video metadata, experimenting with software, and seeking out better search techniques. In the course of this work, they have uncovered videos of intelligence value from a number of countries - and this may be just the tip of the iceberg!

(U) The Technology

(S//SI) The newest camera cell phones make use of "3G" (for "third generation") technology, which is capable of very high rates of data transfer. It can be used for sending video phone-to-phone, phone-to-email, or email-to-phone. Some cell phones already on the market can send and receive images of about the same quality that you would see on a standard television broadcast. Here is an example of a video collected in SIGINT, for demonstration purposes:

Video of Saudi airplane (length: 1:30)

(U) How Is It Used by Our Targets?

(S//SI) Our intelligence targets use cell phone video for a variety of purposes. Depending on what the user is trying to accomplish, video may have dramatic advantages over voice or text communication. It may be a cliché, but it is certainly true that a picture can be worth a thousand words.

(S//SI) For example, terrorists may use cell phone video to carry out surveillance of a site they plan to attack, or to film themselves planting and detonating IEDs (improvised explosive devices), for use in their propaganda or training efforts... Businessmen involved in illicit trade may transmit footage of their wares to prospective buyers... Adversaries involved in negotiations may use video to share documents, taking footage of the paperwork and adding voice commentary. Additionally, everyday people within target countries may use their video cell phones to capture breaking events such as terrorist attacks, riots, or natural disasters. Such videos may allow us to get views of these events not available via the news media.

(U) Finding the Videos

(S//SI) The VCR Pod found cell phone videos sent as e-mail attachments (ports 25 and 110) and as web downloads (ports 80 and 8080) in the PINWALE database. So, how can analysts identify such transmissions in their targets' traffic?

- The e-mail attachments use video-format file extensions, such as .3gp, .3gpp, .3g2, .mpeg4, .mp4, or .amc. The majority of the Pod's examples are of .3gp. A word of warning, though: In addition to videos of intelligence value, these videos often include commercial advertisements, TV and movie clips, home movies, and pornography. Video attachments sent directly from a cell phone are usually accompanied by a very brief text message or no text at all.

- Task cell phone numbers in CADENCE, and search on cell phone numbers of interest in PINWALE. Search in PINWALE for email addresses with "MMS" in their domain names, e.g. 12345@mms.mobitel.si. MMS, or multimedia messaging service, is similar to SMS, but instead of sending short text messages, the user sends images, videos, or other documents. The VCR Pod has compiled a list of MMS domain names used by service providers around the world. PINWALE searches will reveal cell phone numbers in the TO and FROM address lines or the subject lines of email messages.
- Search in PINWALE for terms unique to camera cell phone video files. These include ftyp3gp and Content-Type: video/3gpp.

(U) Automating the Analysis

(S//SI) To help automate analysis as much as possible, the Pod is testing various commercial and research tools to see if they can help single out the golden nuggets of intelligence value. For example, tools exist to carry out face recognition, de-duping, and speech-to-text conversion. Pod members are also developing tools and methods for filtering and sorting videos; this will be particularly useful in filtering out pornography which is often accompanied by banners, etc.

(U) Next Steps

(S//SI) If your office has come across videos of interest or has ideas on how to exploit these signals, Pod 40 members would be happy to collaborate with you. In addition, the Pod offers some training for analysts on how to target and analyze cell phone videos.

(S) You may be asking "What is a Pod, anyway?" Established in January 1997, the S3T1 Pod Research Program is run under the auspices of the SID Technical Advocate Office led by [redacted] *Pods are 6-18 month long, full time teams focused on research into a variety of topics of interest to the Agency that are expected to be a major impact on the Agency's current and future efforts. Pod participants are drawn from throughout the NSA community. Try "go pods" in a browser for more information.*

(U//FOUO) Pod 40 is scheduled to run through February 2007. It always needs new members. Maybe you should consider joining! Please contact the people below.

Dan Aldridge & [redacted]
Co-leaders of Pod 40
[redacted](s)
[redacted] [redacted]

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."
