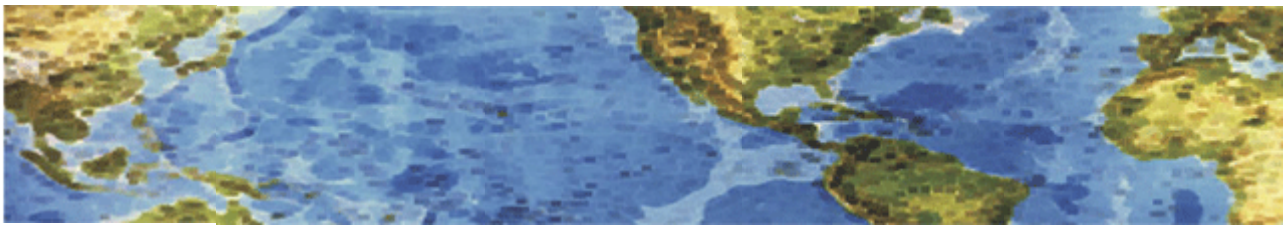
HALL ASSOCIATES



Risk-Based Decision Making Commentary
21 August 2013 Newsletter

Baby-monitor hacker spies on and swears at sleeping 2-year-old

A hacker took over a baby monitor in a home in Houston, Texas, to spy on a 2-year-old girl, to broadcast obscenities at the child, to swivel the camera so as to watch her shocked parents as they came in, and to then call the parents insulting names. According to ABC News, Marc Gilbert and his wife, Lauren, heard the voice of a strange man with a British or European accent coming from the bedroom of their daughter, Allyson, on 10 August. As the parents approached the room, they heard the hacker call their daughter an "effing moron." The voice also told her to "'wake up, you little sl*t."

When the Gilberts entered the room, the monitor's camera swiveled toward them. The hacker then called Marc Gilbert a "stupid moron" and Lauren Gilbert a "b*tch". Marc Gilbert disconnected the monitor and tried to figure out what had happened, but he couldn't, of course, see the hacker - he could only hear the voice and see that the intruder was controlling the camera. Gilbert told reporters that he believes the hacker hacked his router. The hacker also, apparently, hacked the camera, through which he could see Allyson's name on the bedroom wall above her bed. His router was password-protected, and the firewall was enabled. The IP camera was also password-protected.

ABC News subsequently drove through a neighborhood with a baby monitor video receiver on the dashboard, picking up crystal-clear video feeds left and right. First they found Dominic, playing with his toes in his crib. Next they viewed 14-month old Tally, sleeping in her crib. They found a camera pointed at a bed in one neighborhood, and they viewed a woman making a bed in another.

Baby monitors open the home to invasions by creeps and, potentially, burglars in this manner because they're on fixed frequencies, putting out a signal as long as the device is on. The wireless channels used by the devices can often be picked up outside the home, as demonstrated by ABC News when it scanned neighborhoods to see what it could pick up. The vulnerability of these leaky systems was highlighted in 2009 when a US family in the state of Illinois sued the manufacturer of a baby monitor they purchased at toy retailer Toys R Us. After a month of using the monitor, a neighbor warned the family that its camera was broadcasting its signal into their home, enabling the neighbors to hear entire conversations within the nursery. Of course, devices may well be protected by passwords, but default passwords that haven't been changed are like having no password at all. Video baby monitors can broadcast to TVs, hand-held receivers, or even over WiFi to PCs or smartphones. That means you and sometimes others, can keep an eye on your children from almost anywhere. Be careful with these devices' security. That starts with changing default passwords.

http://nakedsecurity.sophos.com/2013/08/14/baby-monitor-hacker-spies-on-and-swears-at-sleeping-2-year-old/

HALL ASSOCIATES

New Android Malware Found

Perkele is a cyber crimeware kit designed to create malware for Android phones that can help defeat multi-factor authentication used by many banks. In this post, we'll take a closer look at this threat, examining the malware as it is presented to the would-be victim as well as several back-end networks set up by cybercrooks who have been using mobile bots to fleece banks and their customers. Perkele is sold for $1,000 (remember my newsletter note on the ongoing malware marketplace), and it's made to interact with a wide variety of malware already resident on a victim's PC. When a victim visits his bank's Web site, the Trojan (be it Zeus or Citadel or whatever) injects malicious code into the victim's browser, prompting the user to enter his mobile information, including phone number and OS type.

That information is relayed back to the attacker's control server, which injects more code into the victim's browser prompting him to scan a QR code with his mobile device to install an additional security mechanism. Once the victim scans the QR code, the Perkele malware is downloaded and installed, allowing the attackers to intercept incoming SMS messages sent to that phone. At that point, the malware on the victim's PC automatically initiates a financial transaction from the victim's account.

Web site security firm Versafe located a server that was being used to host malicious scripts tied to at least one Perkele operation. The company produced a report (PDF), which delves a bit deeper into the behavior and network activity generated by the crimeware kit. If you are interested in the technical details, check out http://krebsonsecurity.com/wp-content/uploads/2013/08/Versafe-SOC-Mobile-attacks-summary-1.pdf

There seems to be a great deal of interest in the cybercrime underground market for developing or procuring tools to trojanize Android devices. According to a recent report from security firm Trend Micro, the number of malicious and high-risk Android apps steadily increased in the first six months of 2013. According to Trend, the number of malicious and high-risk apps took three years to reach 350,000, a number that has already doubled in just the first half of 2013.

Fortunately, a modicum of common sense and impulse control can keep most Android users out of trouble. Take a moment to read and comprehend an app's permissions before you install it. Also, consider downloading and installing apps only from Google's Play store, which scans all apps for malware. This isn't perfect, but they do scan all apps posted. Also there are numerous free and paid anti-malware applications available for Android. All Android devices should be protected.

http://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/