ACC Threat Information Fusion Cell

Homeland Defense Information Summary - 4 November, 2009

Headquarters Air Combat Command
Langley AFB, VA. 23665

General Awareness/Safety Information

(U//OS) Free Download Turns Blackberry into Remote Bugging Device

Source: http://www.theregister.co.uk/2009/10/22/rim_blackberry_bugging_software/print.html)

ACC TIFC BLUF: A free software application for BlackBerry smart phones has the potential to turn the device into a remote listening device that can activated unbeknownst to people in the vicinity of the phone. This further underscores the need to limit access of devices like this in secure areas or areas where sensitive conversations are taking place.

- (U//OS) A free software program released Thursday turns everyday BlackBerry smart phones into remote bugging devices. Dubbed PhoneSnoop by creator Sheran Gunasekera, the software sits quietly on a targeted BlackBerry and monitors the phone number of each incoming call. When it detects a number set up in the program's preferences section, it silently turns on the speakerphone, allowing an attacker to monitor all conversations within earshot of the device. Although programs such as FlexiSPY (http://www.flexispy.com/) have long claimed to do much the same thing, Gunasekera said he believes PhoneSnoop is the first software to bring those capabilities to the BlackBerry free of charge. "What I wanted to do was bring some awareness to this problem, so I'm releasing it pretty much for free and trying to show them that this can be done," said Gunasekera, who is director of security for Hermis Consulting in Jakarta, Indonesia. "It's not well known that these threats exist." Gunasekera said he was inspired to write PhoneSnoop after witnessing an attempt in July by United Arab Emirates mobile operator Etisalat to sneak snooping software onto customers' Blackberry handsets. Subscribers reported receiving an SMS message from the carrier instructing them to install an official patch. An analysis and reverse engineering of the update made it clear that the update installed a program that had the ability to forward all outgoing emails to a server under Etisalat's control, Gunasekera said. He added that it's not known if the spyware was ever activated. Because the software cloaked itself from users, it may never have been discovered were it not for a bug that drained batteries in as little as 30 minutes. The carrier denied the software spied on its customers, but even BlackBerry maker Research in Motion warned users of the SMS message and took the unusual step of offering an application that removed the Etisalat software. Unlike FlexiSPY and the spyware that was installed on Etisalat customers' handsets, PhoneSnoop doesn't try to hide itself. But Gunasekera said it would be trivial for him to modify the program to hide all its processes and icons from casual users. He plans to release a free utility in a week or two that will make it easy for users to list all software and processes running on their BlackBerries. PhoneSnoop complements a previous program Gunasekera released at this month's Hack in the Box security conference that silently forwards emails to an attacker. Eventually, he plans to release companion software that will forward all SMS messages and monitor a user's location using the BlackBerry's built-in GPS features. Unlike Apple's iPhone and other smartphones, the BlackBerry hasn't suffered from known vulnerabilities over the past couple of years that would allow an attacker to remotely install snooping software onto the device. That means attackers need physical access to the device they want to bug or somehow trick its user into installing it. But those scenarios are by no means out of the question, as Etisalat customers know all too well.

Possible Surveillance/Reconnaissance Activity

(U//FOUO//LES) Suspicious Photographing of Synagogue – Baltimore, Maryland

(Source: Maryland Coordination and Analysis Center Daily Summary, 3 Nov 09; Guardian Record ID: 134920 BA)

ACC TIFC BLUF: Possible surveillance of Baltimore religious facility. According to a May 2007 DHS report on Religious Facilities, there are approximately 250,400 religious congregations consisting of about 138 million members in the U.S. These congregations represent approximately 200 different religions. For a threat actor intent on attacking a religious facility, vulnerabilities are many and include a significant number of people of like faith gathered in a single location at a specified time; unrestricted access to religious services; unrestricted access to peripheral areas of the facility; limited or non-existent security; and access by workers/maintenance staff with little or no background checks.

- (U//FOUO//LES) On 2 November 2009, the FBI Baltimore Field Office received information regarding the suspicious photographing of a synagogue located in Baltimore, MD. The complainant stated that he witnessed two males who appeared to

be photographing the Synagogue and the adjoining pre-school. The subjects were in an identified white mini-van displaying a Wisconsin registration.

Suspicious Activity/Tests of Security

(U//FOUO//LES) Suspicious Activity/Incidents Involving the Los Angeles Metrolink

(Source: 29 Oct 09 LAJRIC/RTTAC Report; LA JRIC Weekly Digest, 21-27 Oct 09; LAJRIC Daily, 28 Sep 09)

ACC TIFC BLUF: Multiple suspicious incidents, to include possible surveillance and activities which *appear* to be "dry-runs" have been reported to Los Angeles law enforcement personnel. Although there is no DoD nexus, the activity itself, and the prompt reporting by concerned citizens, serve as good examples for the rest of us to follow. Situational awareness and prompt reporting are key factors in the prevention of terrorism.

- (U//FOUO//LES) Possible Surveillance of Transportation Infrastructure, Los Angeles, California: On 26 OCT at approximately 1400 hours, a private citizen was waiting for an eastbound train inside of the Metro Red Line Station, located at Vermont Avenue and Sunset Boulevard. The citizen observed an adult male photographing the tunnel and the surveillance cameras in the area. The reporting party stated that the suspicious individual did not board the train when it arrived at the station.
- (U//FOUO//LES) Suspicious Subjects with Backpacks Board Red Line Train, Los Angeles, California: On 23 October, a concerned citizen approached a Los Angeles SD Deputy working at the bag screening area of Union Station. The citizen stated that at approximately 0640 hours, he observed two adult males, each with backpacks and talking as if they knew each other very well, at the Wilshire/Vermont station for the red line train. Both males seemed very nervous and looking in all directions as they waited for the train. When the train arrived at the station, the two males separated and entered onto the train, one then the other. They did not sit together and continued to act nervous as they sat at each exit door. Both males held onto the backpacks in a careful manner with both hands. When the train arrived at 7th/Metro station, both males stood up and exited the train at different times. The deputy has requested the video of both the platforms and trains between the hours of 0630-0700 hours where the individuals were observed.
- (U//FOUO//LES) Suspicious men on Metrolink train. A private citizen reported to the Los Angeles Sheriff's Department of three suspicious men on the subway at 7th and Metro at approximately 0530 hours on 24 SEP. He stated that he saw one man looking very nervous. The man moved to another platform when he saw the caller looking at him. He then noticed two other men with bags who were all making eye contact before getting on separate cars on that train. The caller then waited for the next train and noticed three more men sitting on a bench facing the train that had just left, which was odd since they didn't get on the train. They all got up at the same time as the train left and turned to get on a train coming in the opposite direction. They were all carrying bags and got on separate cars. The caller thought it was odd that they were facing a different train and waited for it to leave before entering another train.

(U//FOUO//LES) Suspected Drug Traffickers Using Fake Military IDs.

Source: State of Iowa Intelligence Fusion Center

ACC TIFC BLUF: The use of fake military identification, most likely intended to add a measure of credibility in the event the perpetrators were stopped and questioned, demonstrates the lengths some will go to carry out their criminal endeavors. To the best of our knowledge, there is no DoD ID card in this particular format. (If anyone knows otherwise, please advise.)

(U//FOUO//LES) Two US Persons suspected of drug trafficking following a traffic stop on 10/26 by the Iowa State Patrol on I-80, presented fake military identification cards possibly in an effort to cover their illicit activities. A K-9 unit alerted on the subjects' vehicle and during a subsequent search several empty suitcases were located that a 'strong odor of marijuana.' Two bags were found containing 21 bundles of cash that totaled $148,865. The money was seized. The military ID USPER1 presented to the trooper indicated he was a major in the U.S. Army Special Forces and USPER2's ID stated he was a Staff Sergeant with the Special Forces. Troopers also noted that military uniforms were hanging in the back of the Ford Explorer the subjects were in along, with a military bag. Both subjects had California DLs and were en route from Chicago or Cleveland (their stories varied) to San Francisco. Currently the subjects' intent for possessing the fake military IDs along with the legitimate military uniforms is unknown but the investigation is ongoing. Law Enforcement Response: Agencies with information on this or other instances of fake military, police, or other official identifications are asked to contact the State of Iowa Intelligence Fusion Center at (800) 308-5983 or via email at ialein@mocic.riss.net.

ACC Threat Information Fusion Cell

Homeland Defense Information Summary - 4 November, 2009

Headquarters Air Combat Command
Langley AFB, VA. 23665

General Awareness/Safety Information

(U//FOUO//LES) Portable GPS and Cellular Jammer.

Source: MCAC 6 Nov 09; North Vancouver RCMP OFFICER SAFETY Bulletin, NVAN 2009-26354;

ACC TIFC BLUF: If activated, the device is capable of jamming portable radios, and possibly cell phones, within 30 feet.

- (U//FOUO//LES) **Portable GPS and Cellular Jammer.** On 09/15/2009 at approximately 0208 hours, Police stopped a vehicle on Highway 1 westbound, and identified USPER1 as the driver of the vehicle and USPER2 as the passenger. Police immediately smelled a strong odor of burnt marijuana coming from the vehicle. A Police K9 unit was dispatched and a search of the vehicle was completed. Police located a small amount of marijuana. Police also located a Portable GPS and Cellular Jammer in the center console of the vehicle. USPER1 could not provide Police with an explanation as to why he was in possession of the device. USPER1 stated that he purchased the device for $120.00 at a flea market in Surrey. USPER1 would not provide any further details. The device had been turned off at the time Police located it. Police turned the device on and found that their portable radios would not transmit within 30 feet. This included the emergency 10-33 button. USPER1 relinquished the device to the Police.

Suspicious Activity/Tests of Security

(U//FOUO//LES) Individual Claiming to Be an Airline Pilot Arrested

Source: TSA TSIR, 4 November 2009

ACC TIFC BLUF: The use of official uniforms and/or vehicles is rapidly becoming a standard TTP for terrorists and criminals and takes advantage of the fact that "official" persons and/or vehicles often reduce the inquisitiveness/suspicious nature of security personnel.

- (U//FOUO//LES) October 20, 2009 – A TSA travel document checker at Newark Liberty International Airport observed a passenger attempting to circumvent the screening checkpoint. The passenger, who was wearing a U.S. Navy service uniform, claimed he was an El Al pilot. The individual did not have airline identification and presented a military identification card, which was later determined to be invalid. The passenger returned to the same checkpoint a short time later and attempted to gain access to the sterile area again, but this time by claiming he was with a group of Lufthansa air crew members. When a TSA behavior detection officer engaged the passenger, the passenger claimed he was an El Al pilot on a classified mission. Port Authority Police and TSA federal air marshals interviewed the passenger who continued to claim he was on a classified mission. Additional screening revealed a kubaton and a knife inside his carry-on bag. The Naval Criminal Investigative Service verified the passenger previously served in the U.S. Navy, but was currently on Inactive Reserve status. The passenger was subsequently arrested on state charges of "Possession of a Weapon" and "Criminal Impersonation." **TSA Office of Intelligence Comment:** While the passenger's intent is not clear, the method used in his attempt to circumvent security screening is of concern. According to the FBI, impersonation has been a feature of many terrorist attacks overseas. Terrorists have used the uniforms and identification of military, law enforcement, airport, delivery service, and emergency services personnel to gain access to attack sites, to transport weapons, and to conduct preoperational surveillance and planning. Uniforms could be acquired by theft, counterfeit manufacturers, or purchased over the Internet.