ROLL CALL RELEASE

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

1 May 2013

(U//FOUO) Increasing Exploitation of Mobile Device Vulnerabilities

(U//FOUO) State, local, tribal and territorial (SLTT) computer networks have been increasingly targeted by cyber adversaries. At the same time, the expansion of mobile devices integrated into SLTT networks provides new opportunities for cyber adversaries seeking to collect information or disrupt operations by compromising mobile technology and exploiting vulnerabilities in portable operating systems, application software, and hardware. Compromise of a mobile device can have an impact beyond the device itself; malware can propagate across interconnected networks.

- (U//FOUO) Sensitive information available on mobile devices—both professional and personal—represents an attractive target for malicious cyber actors for a variety of reasons, including criminal activity and identity theft, collection of SLTT agency information, and disruption of communications.
- (U//FOUO) Mobile devices contain information not typically found on a personal computer, such as global positioning system (GPS) information and text messaging. Commercial spy software could provide a cyber actor with the capability to secretly read text messages, call logs, e-mails, and view a phone's GPS location.

(U//FOUO) Threats to mobile devices are evolving beyond attacks on software to include targeting of hardware components within devices. Exploits targeting hardware are more complex and require a higher level of expertise, but can provide cyber actors with significantly higher levels of access and control.

- (U) In May 2012, a posting to Pastebin.com revealed the existence of a backdoor on a popular Android-based smartphone manufactured by the Chinese technology company ZTE and sold exclusively in the United States, according to US press. The vulnerability allows anyone with the password—which was hard-coded into the processor and widely available online—to gain root access to the device. ZTE acknowledged the vulnerability and stated they were actively working on a security patch, which has yet to be released.

(U) Potential Indicators of Compromised Mobile Devices

(U) Two or more of the following, occurring simultaneously, may indicate a compromised mobile device:

- (U) Abnormally short battery life of mobile device, even after a complete recharge;
- (U) Activated secondary communication protocols (Bluetooth, infrared, etc.) that were not enabled by the user;
- (U) Inability to power-down or turn off device; and
- (U) Unexplained unavailability or malfunction of mobile device features.

(U) Protective Measures

(U) The following preventive measures could reduce the likelihood or consequences of mobile device exploitation:

- (U) Use of strong passwords for device access;
- (U) Download only applications authorized by network administrators;
- (U) Disable interfaces (Bluetooth, Wi-Fi, infrared, etc.) not actively in use; and
- (U) Maintain physical control of device.

(U) Report Suspicious Activity

(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.

IA-0111-13