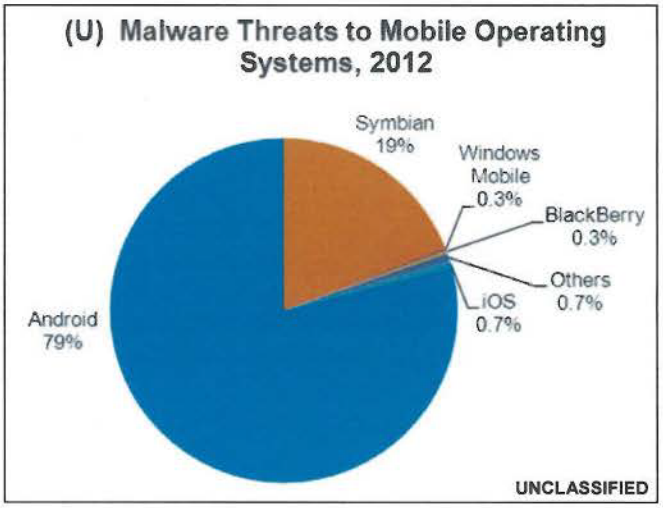
ROLL CALL RELEASE

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

23 July 2013

(U//FOUO) Threats to Mobile Devices Using the Android Operating System

(U//FOUO) Android is the world's most widely used mobile operating system (OS) and continues to be a primary target for malware attacks due to its market share and open source architecture. Industry reporting indicates 44 percent of Android users are still using versions 2.3.3 through 2.3.7—known as Gingerbread—which were released in 2011 and have a number of security vulnerabilities that were fixed in later versions. The growing use of mobile devices by federal, state, and local authorities makes it more important than ever to keep mobile OS patched and up-to-date. The following are some known security threats to mobile OS and mitigation steps.



Security Threat	Description	Mitigation Strategy
SMS (Text Message) Trojans represent nearly half of the malicious applications circulating today on older Android OS.	Sends text messages to premium-rate numbers owned by criminal hackers without the user's knowledge, potentially resulting in exorbitant charges for the user.	Install an Android security suite designed to combat these threats. These security suites can be purchased or downloaded free from the Internet.
Rootkits are malware that hide their existence from normal forms of detection. In late 2011, a software developer's rootkit was discovered running on millions of mobile devices.	Logs the user's locations, keystrokes, and passwords without the user's knowledge.	Install the Carrier IQ Test—a free application that can detect and remove the malicious software.
Fake Google Play Domains are sites created by cybercriminals. Google Play enables users to browse and download music, books, magazines, movies, television programs, and other applications.	Tricks users into installing malicious applications that enable malicious actors to steal sensitive information, including financial data and log-in credentials.	Install only approved applications and follow IT department procedures to update devices' OS. Users should install and regularly update antivirus software for Android devices to detect and remove any malicious applications.

UNCLASSIFIED

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0166-13