FCC TAC SECURITY & PRIVACY WORK GROUP
LONGER TERM ANTI-MALWARE RECOMMENDATIONS

INTRODUCTION

This brief paper describes the Security and Privacy Work Group's longer term recommendations which are intended to look beyond the actionable items related to end user education and Wi-Fi security. These longer term recommendations attempt to address the growing problems of malware and malicious applications targeting consumer and enterprise devices. In particular, the Work Group feels the threats related to mobile devices have the greatest need for action. These recommendations take the form of fostering collaborative initiatives across industry stakeholders. This will engender a cohesive and systematic approach to counter the looming crisis around mobile device security.

A GROWING REASON FOR CONCERN

The reality is the smartphone has become the information hub, and this role is increasing. The number of smartphone apps is rapidly growing, and the trend is for more connectivity and processing of greater amounts of sensitive information. This is driven by the growing use of online banking, e-wallet, corporate email, local file storage, location tracking services, social networking, direct device-to-device communication, etc. Most of these mobile devices regularly use unsecured public Wi-Fi hotspots to exchange this information, with little regard by most consumers for the significant security implications.

As a result of this information hub trend, the smartphone has become a very rich and highly vulnerable attack target. Several industry studies have shed light on this trend, including a recent statement from Security research firm Kaspersky Labs[1], which stated the volume of new Android malware increased 3X in 2Q 2012, and a similar report from Trend Micro[2] that the number of malicious Android apps doubled from 10,000 to 20,000 in just one month that same quarter. The threats are not just in the form of otherwise benign applications being infected with malware, but also in the form of malicious applications populating application stores. According to RSA[3], mobile applications have emerged as an important cyber crime attack vector for phishing and malware.

Yet, as the threats increase in magnitude and sophistication, there is not a corresponding increase in the application of threat mitigating mechanisms. A September 2012 report by Juniper Research[4] indicated only 5 percent of smartphones and tablet devices have any form of security software installed. The extraordinarily rapid rate at which phones have transformed into always-on (often Enterprise-connected) general purpose handheld computers, and attractive as mobile platforms for many types of commerce, also makes them very attractive

[1] http://www.kaspersky.com/about/news/press/2012/Android_Under_Attack__Malware_Levels_for_Googles_OS_Rise_Threefold_in_Q2_2012

[2] http://www.trendmicro.co.uk/newsroom/pr/the-true-face-of-the-android-threat

[3] http://www.emc.com/about/news/press/2012/20120725-01.htm

[4] http://juniperresearch.com/viewpressrelease.php?pr=339

targets for cyber crime. As the mobile devices have settled into two major operating systems (Apple IOS and Google Android) and two second tier OS (RIM and WINDOWS), bad actors have benefited from the "standardization" of platforms to help focus attacks against popular applications and platforms.

Only an end-to-end and collaborative effort, with both proactive and reactive elements, will make any meaningful progress toward this rapidly growing problem. On the consumer side, this effort must holistically address consumer education. On the industry side, there is a need to increase synergy and coordination across the ecosystem (network services, devices/platforms, applications), by fostering existing and new industry/government partnerships, and by creating new opportunities for information sharing across industry stakeholders.

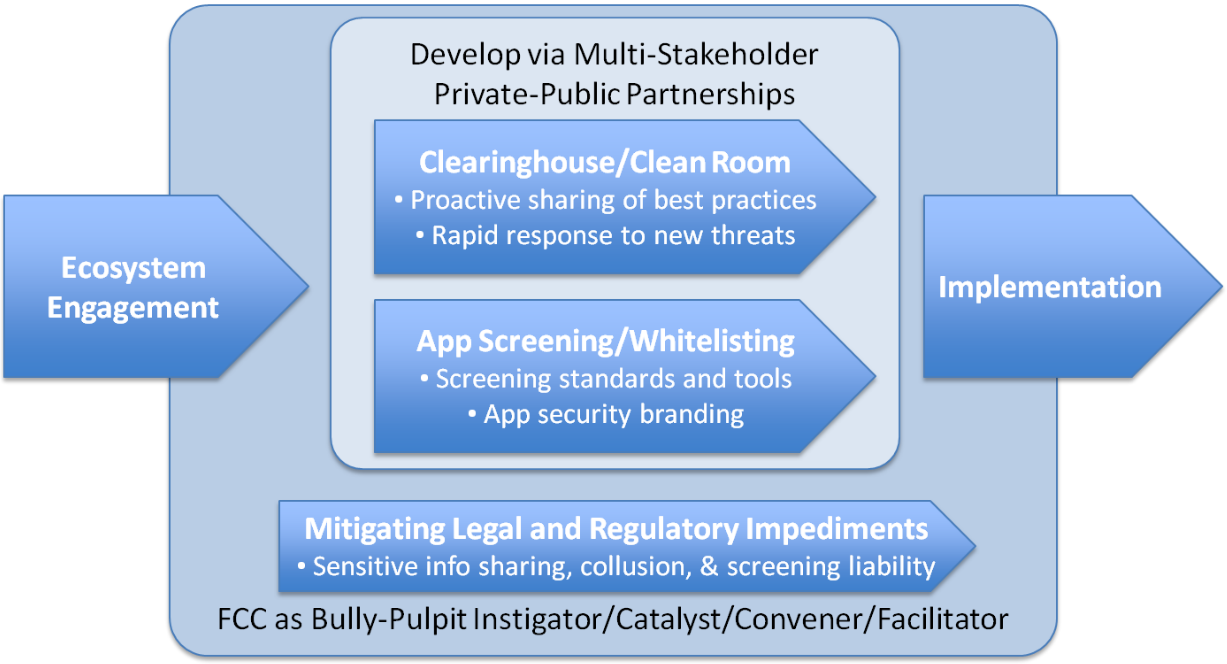
RECOMMENDATIONS

No single industry segment can solve the rapidly expanding mobile malware problem. Not only is an industry wide approach needed, but no single action will make any meaningful progress. A combination of government/industry collaboration, and an actionable plan that consists of multiple, diverse approaches in unison, is needed in this space for meaningful progress.

Specifically, our recommendations are centered on two initiatives:

- a **clearinghouse/clean room** approach for information sharing and response development
- an **application screening/whitelisting** initiative that allows applications to be evaluated and 'branded' for security

These initiatives are depicted in the figure below in context with the major activities required to execute on them.



Ecosystem Engagement

Develop via Multi-Stakeholder Private-Public Partnerships

Clearinghouse/Clean Room
- Proactive sharing of best practices
- Rapid response to new threats

App Screening/Whitelisting
- Screening standards and tools
- App security branding

Implementation

Mitigating Legal and Regulatory Impediments
- Sensitive info sharing, collusion, & screening liability

FCC as Bully-Pulpit Instigator/Catalyst/Convener/Facilitator

A **clearinghouse / clean-room** initiative is recommended to facilitate greater synergy and information sharing between industry ecosystem stakeholders. A neutral, government facilitated organization is viewed as the best way to bring together industry partners and competitors alike. Such an organization could take inspiration from the well known federal agency chartered with proactive and reactive actions associated with "human malware" –

the Centers for Disease Control and Prevention (CDC). The CDC, among other roles, is chartered with fostering timely information sharing across various health related organizations and entities. The CDC's Situational Awareness Section[5], in particular, may serve as a model for information sharing and incident response for the space of mobile device malware. It is worth noting that the same forum could be used by ecosystem providers to deal with malicious/coordinated cyber attacks (threat identification/classification, development of response tactics, implementing response and development of future defense mechanisms).

The clearinghouse / clean-room will specifically enable sharing of information on malware, new device/OS/app vulnerabilities, application blacklists, incident response, etc. As part of this activity, detection methodologies and counter-threat mechanisms will be devised and disseminated. The initiative should include representatives from carriers, OS vendors, application stores, anti-malware providers, and application vendors. This forum should also look to access the best information and practices available and will likely find it beneficial to reach to other entities, such as government agencies and academia, which bring specific expertise and/or assets in this area. A balance must be made between complete inclusion of all stakeholders, and the desire for rapid response and dissemination of information. It may be advisable to limit membership to a core set of stakeholders, while facilitating the publication of actions/recommendations to a much broader community.

The **application screening/whitelisting** approach focuses on helping the consumer to better appreciate the growing threats from malware by providing them with a friendly and easy way to be vigilant against security threats. This centers on the provision of a security 'brand' or 'seal of approval' that would be assigned to validated and certified applications. By developing guidelines for apps stores and OS vendors that convey a security 'brand' consistently, consumers will receive some level of assurance on application safety, regardless of which vendor supplies the application.

Consistent security branding is seen as a powerful and concise tool for enabling end users to assess the security concerns associated with installing particular applications. If branding can be implemented in way that establishes a minimum level of vetting for a given "secure" label, end users can have some sense of ease that the application will only perform the intended functions. This branding is somewhat analogous to appliances earning certification by Underwriters Laboratories. The UL label conveys a minimum set of testing has been applied to the device, providing some level of assurance of functionality only as intended by the user. The UL analogy can be used as part of consumer education as well, to help with the understanding of the branding objectives. Exploring secure branding further, there is the possibility for tiered branding to represent higher levels of vetting (e.g. an "Enterprise grade" stamp of approval, possibly with a correspondingly higher initial purchase/subscription prices).

While security branding alone does not sufficiently address all the issues raised here, it is viewed as an important part of a holistic approach to the problem. The Security and Privacy Work Group's shorter term recommendations on end user education, along with security branding, and increased availability of consumer tools that facilitate real time communication of malware incidents, are seen as the key elements in a multi-faceted approach to engaging the consumer. Without some level of consumer engagement, the end user will be by far the weakest link in the security chain.

[5] http://www.bt.cdc.gov/situationawareness/

EXECUTION SUGGESTIONS

With reference to the previous figure, the Security and Privacy Work Group recommends the following 4 phases of execution.

Ecosystem Engagement

- Engage industry players (Carriers, Mobile OS/Platform Providers, Security/Anti-Malware Services) to set the overall direction and leverage the FCC bully pulpit as needed, to garner engagement by reluctant stakeholders.
- Engage CERT to help establish best practices for defense, reporting, and response.
- Identify competitive and legal (e.g., collusion, liability, etc.) issues that impede collaboration among industry players

Development

- Work with the National Institute of Standards and Technology (NIST) to develop application screening and labeling guidelines, by leveraging their existing work on mobile device security / BYOD guidelines (e.g. SP 800-124), and malware incident prevention/handling (e.g. SP 800-83). Screening efforts/guidelines need to address two types of threat categories: 1)intentional malware disguising as legitimate applications, 2) non-malware that contains flaws which allow other entities to exploit it
- Work with US-CERT to leverage their expertise on software assurance and malware code analysis to foster screening tool development, and include the creation of new screening tools, and certification of existing vendors' app store screening
- Establish an application security branding mechanism and a minimum set of malware screening guidelines for secure branding within app stores
- Create consistent sandboxing guidelines to help limit damage from illicit applications
- Develop recommendations to standardize implementations/interfaces for network and device interfaces intrinsic to security. Further NIST's work (SP-800-164 Hardware-Rooted Security in Mobile Devices)
- Define a feedback process from users, anti-malware services, and screening tools that identifies malware as well as illicit applications and network services.
- Define an application whitelisting process that feeds back incident response information into timely updates
- In support of consumer engagement, develop shorter term recommendations that would enhance end user education effectiveness:
  - security branding
  - increased availability of consumer tools that facilitate real time communication of malware incidents
  - common definitions and labeling of security settings across different operating systems
  - common, robust default settings across different operating systems and applications

Implementation

In general, the work products emanating from the aforementioned development activities should be rolled out in a phased fashion, which best aligns with resource availability within the FCC, NIST, US-CERT, and key industry stakeholders.

- Execute on the clearinghouse / cleanroom model of industry information sharing and incident response
    - Model after the Centers for Disease Control and Prevention (CDC) - specifically the CDC's Situational Awareness Section for information sharing and incident response
    - Enable sharing of information on malware, new device/OS/app vulnerabilities, application blacklists, incident response, etc.
    - Engage industry experts in threat identification and response
    - Include representatives from carriers, OS vendors, apps stores, anti-malware providers, and application vendors.
    - Strike a balance between complete inclusion of all stakeholders, and the desire for rapid response, by limiting the clearinghouse to a core set of stakeholders, while facilitating the publishing of actions/recommendations to a much broader audience.
- Execute on application screening/whitelisting
    - End user awareness / education campaigns and collateral
    - Carrier and Application Store implementation of screening and application brand management practices (screening, blacklisting, updates to respond to threats)

Mitigation of Legal and Regulatory Impediments

As part of industry engagement, care must be taken to address the non-trivial legal challenges surrounding the sharing of sensitive information between industry partners and competitors. Companies must feel unencumbered to share incident data, forensics, application blacklists, etc., without concern of arming competitors with proprietary or embarrassing information. Just as important is addressing concerns about the appearance of collusion between competitors, and the resulting potential violation of U.S. antitrust laws. The CDC analogy applies here as well, with the leveraging of the concept of "clean rooms", where important information can be collected in a way that removes "contaminants" such as company specific data, or any information deemed as an enabler for collusion. Similarly, companies will be concerned about any implied liabilities that might stem from this work (e.g., branding an application as 'secure' that later proves to contain a security breach resulting in negative consequences for some user community). The Work Group feels that only a federal government entity can adequately address these competitive, regulatory and legal concerns.