Government Business Council
Briefings

A Briefing
from GBC's:
Research Analysts
March 2013

3 Mobile Security Threats A BYOD Strategy Should Prepare For

As government works to keep up with the mobile revolution, more and more applications are becoming available on personal devices. Several agencies are operating bring-your-own-device (BYOD) policies, including the General Services Administration (GSA), Nuclear Regulatory Commission (NRC) and National Aeronautics and Space Administration (NASA), while others are enabling more mobile transactions for citizen services. The Department of Veterans Affairs (VA), for example, will soon allow veterans to access their medical information via smartphone or tablet.

While these programs present agencies with an opportunity to make more transactions mobile and potentially decrease IT costs, they may also make the agency vulnerable to security breaches. One of the biggest threats is social engineering, a process by which an adversary tricks the user into offering up information or access rights. When used to attack mobile devices containing sensitive professional applications like email, social engineering can pose a large threat to security. Proper precautions are needed as federal agencies move forward in expanding their mobile strategies.

> "Though government agencies invest large sums of money into their IT defenses, an unknowing user can help adversaries dethrone even the most regal of security systems."

What Is Social Engineering?

Social engineering refers to manipulating people into doing things they otherwise would not do. With regard to cybersecurity, it refers to the ability to manipulate users into disregarding normal security precautions, often by opening an SMS or email message with a malicious link. Adversaries behind social engineering attacks may try to gain the trust of the person they are attacking, and frequently use individuals' weaknesses or natural helpfulness against them. After extracting the necessary access information from the user, the adversary is often able to affect other applications residing on the mobile device. Depending on what is stored on the device, and what networks the device has access to, this can result in massive data loss and corruption. Though government agencies invest large sums of money into their IT defenses, an unknowing user can help adversaries dethrone even the most regal of security systems.

Attacks to Watch

There are several types of social engineering to be on the lookout for at your agency, including:

1 Suspicious URLs

Many social engineering attacks begin as phishing messages that download Trojanized applications to your mobile device. Many of these messages appeal to the recipient's desire to get something for nothing, by offering a prize or mobile application without cost. One example is the Android.Pikspam attack. During this attack, users are informed by SMS that they've won a prize or are directed to a free version of a popular mobile application. By clicking a URL, the

> With access to the personally identifiable information of millions of citizens and national security secrets, federal employees must be vigilant about their mobile presence.

end user downloads the desired app, but also unknowingly downloads a Trojanized application that infects the device and then deletes all traces of its installation. The Trojan then has the ability to turn different application components on and off and takes control of the user's contacts. All contacts are sent the original SMS message and the cycle continues, further expanding the adversary's control.

2 Unexpected Security Upgrades

Some phishing attacks gain access to a device and then propose fake security upgrades or maintenance. A recent, elaborate form of this attack is ZitMo (ZeuS-in-the-Mobile), an Android and BlackBerry-based application that bypasses online banking security software and transfers huge sums of money to adversary accounts. ZitMo begins as a phishing message from the victim's bank, asking them to click a link which downloads the Trojan to their PC. The next time the victim logs onto his or her banking account, the Trojan interrupts the webpage and tells the victim to install a security upgrade. By preying upon those used to two-step authentication procedures, the Trojan-controlled webpage asks the user to download software to their mobile device to aid in encryption. If the end user complies, the adversary will gain access to everything needed to bypass the typical two-factor authentication required by banks and can begin transferring money. While ZitMo attacked financial accounts, this type of social engineering could be replicated for any accounts requiring authentication by mobile device.

3 Requests for Information

Phishing is a real threat, but it is not just malicious mobile applications that users need to be aware of. Social media applications, which are expanding in the federal government, can easily be leveraged for social engineering. This may be concerning as every cabinet level agency has both a Twitter and Facebook, and some have even more of a social media presence. Several secretaries have their own public-facing Facebook pages, and the Department of the Interior even uses Tumblr. While social media can be useful to disseminate news and information about events in real-time, it can also put the agency at risk of exploitation. In March 2012, fake Facebook accounts were created of NATO's supreme allied commander Europe (Saceur) Admiral James Stavridis. Authorities found that adversaries involved in this attack were conversing with Stavridis' friends and colleagues hoping to collect personal and professional details.[1]

Social media applications may also transmit data to the company without the user knowing. Legislators are investigating whether social media applications can collect address book information and photos without notifying the user. Some jurisdictions, like California, require mobile developers warn consumers about what information will be collected and how it will be used.[2]

Securing the Future

The threats discussed here are damaging to any citizen, but could make an indelible mark on the United States government. With access to the personally identifiable information of millions of citizens and national security secrets, federal employees must be vigilant about their mobile presence.

One way to do this is provide continuing education to employees. OMB Circular No. A-130 requires that agencies "ensure that all individuals are appropriately trained in how to fulfill their security

responsibilities before allowing them access to the system." It also states that periodic refresher training should be required for continued access to the system.[3]

Despite these precautions, lapses in judgment or forgetfulness are unavoidable. For personal devices to be safely used for federal purposes, agencies should consider pairing ongoing employee education with application restrictions and careful oversight. As agencies debate expanded device and data management policies, creating a divide between personal and professional content is essential.

—By Zoe Grotophorst, Dana Grinshpan (editor)

About F5

F5 Networks makes the connected world run better. F5 helps federal agencies meet the demands and embrace the opportunities that come with the relentless growth of voice, data, and video traffic, mobile workers, and applications—in the data center, the network, and the cloud. The world's largest businesses, service providers, government entities, and consumer brands rely on F5's intelligent services framework to deliver and protect their applications and services while ensuring people stay connected. Learn more at www.f5.com.

About GBC: Briefings

As Government Executive Media Group's research division, Government Business Council Briefings are dedicated to advancing the business of government through insight and analytical independence. The GBC Briefings team conducts primary and secondary research to learn and share best practices among top government decision-makers in the tradition of Government Executive's over forty years of editorial excellence.
For more information, contact Bryan Klopack, Executive Director of Research and Analysis, Government Executive Media Group, at bklopack@govexec.com.

Sources:

1. Nick Hopkins, "China Suspected of Facebook Attack on Nato's supreme allied commander," The Observer, 10 March 2012.
2. Matt Squire, "In California, Mobile Apps Developers Receive Privacy Warning From State AG," Cybersecurity Policy Report, 5 Nov 2012.
3. Appendix III to OMB Circular No. A-130, Feb 1996.