FEDERAL NEWS RADIO.COM

EXECUTIVE BRIEFING SERIES:

Mobile Security

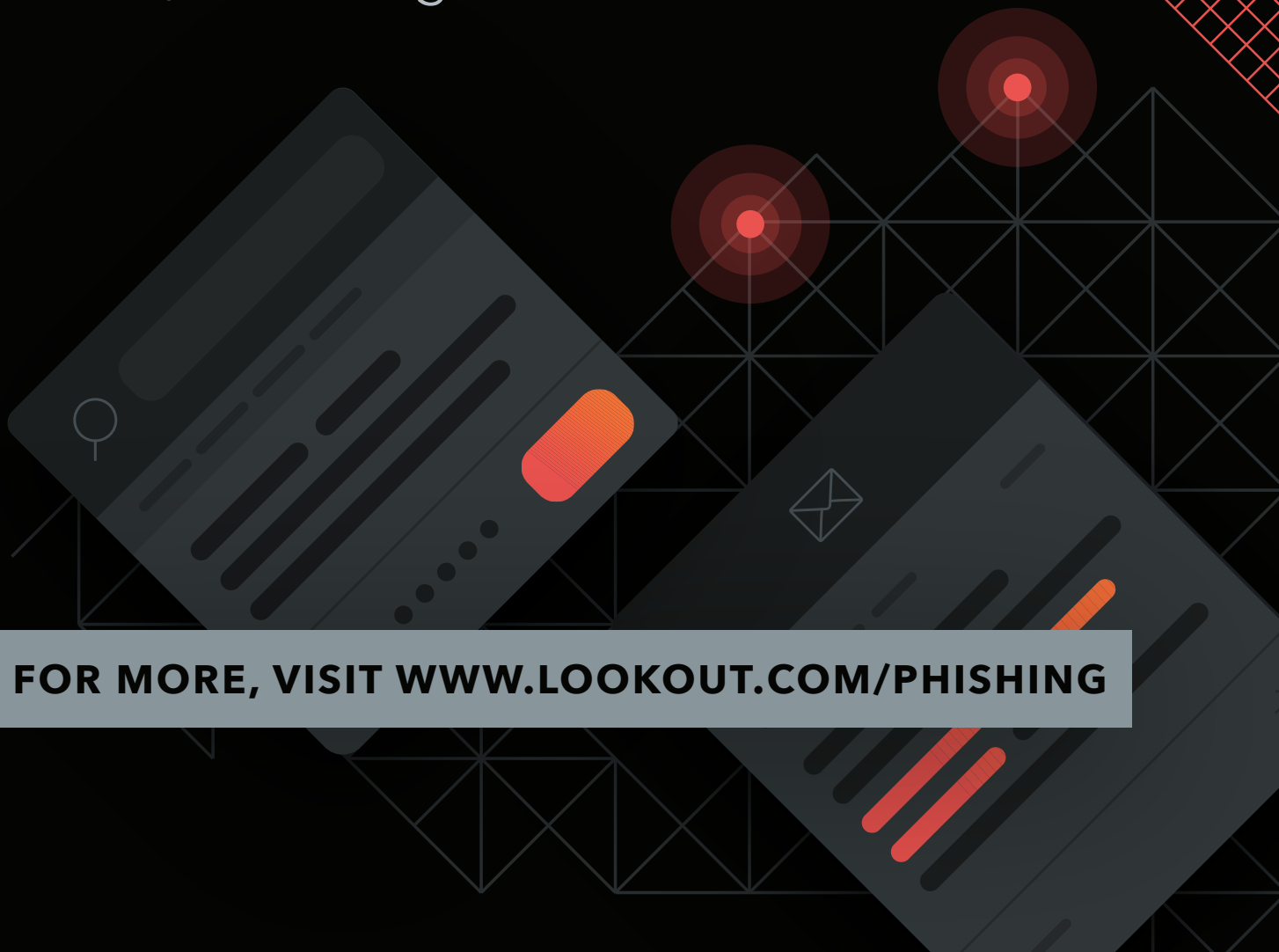
Sponsored by Lookout

Lookout®

MOBILE PHISHING

THE BIGGEST UNSOLVED PROBLEM IN CYBERSECURITY

Mobile users 3x as likely to get phished, according to IBM



FOR MORE, VISIT WWW.LOOKOUT.COM/PHISHING

A Decade in, Mobile Still Presents Unique Security Challenges

BY TOM TEMIN

If one word characterizes mobile computing, it might be "more." More enterprise applications are going mobile. More federal employees are using mobile devices as their main computing hardware, often carrying both a tablet and a smartphone or two. More citizens are accessing more digital services with mobile devices.

Unfortunately, federal agencies also face more mobile malware. More, and more elaborate, phishing attempts arrive at mobile inboxes daily.

Greater volumes of mobile activity and still-growing numbers of mobile devices mean IT and security people must constantly update their approaches to mobile cybersecurity. In fact, mobile, LAN, data center and cloud computing have become so intertwined that mobile security is becoming more integrated with cybersecurity and is essential to an organization's infrastructure.

In other words, your agency's mobile cybersecurity strategy of two years ago likely needs updating.

PANEL OF EXPERTS

Kenneth Bible, Deputy Director, C4/ Deputy Chief Information Officer, U.S. Marine Corps

Brian Depasse, Assistant Director, Cyber Engineering, Architecture and Identity Management, Department of Justice

Christopher Maynard, Acting Director, Office of the Chief Information Security Officer, Governance Executive Management Division, Department of Homeland Security

Joe Ramsey, Chief Information Security Officer, U.S. International Trade Administration

Matt Scholl, Chief, Computer Security Division, Information Technology Lab. National Institute of Standards and Technology

Chris Smith, Vice President, Shared Services, AT&T Public Sector and Wholesale Solutions

Bob Stevens, Vice President, Public Sector, Lookout

To get the temperature of mobile cybersecurity, Federal News Radio and Lookout brought together several federal security and IT practitioners. We asked them their views of the state of mobile cybersecurity and their strategies for dealing with it.

Notwithstanding the degree of integration of mobile devices into IT infrastructures, participants agreed mobile still presents unique cybersecurity challenges.

Needed: Zero Trust

An important theme that emerged is the ongoing need for user training specific to mobility and mobile devices. Joe Ramsey, chief information security officer of the U.S. International Trade Administration, said, "Where I see a huge threat is in the capabilities of the devices themselves, and how we have to educate users on different behavior."

Ramsey said while mobile cybersecurity and all cybersecurity should be integrated, the rise of mobile devices has changed his organization's view of network protection from the "castle-moat" model of the client-server era to a borderless view, where emphasis is on data access controls and device hardening, at least as much as on perimeter protection with firewalls that applies to data centers.

He cited the example of a high-level official moving securely, using a hardened device, then taking a selfie with someone and posting it on the agency's Facebook page with all of the details.

Or perhaps the offending user is the person's executive assistant (EA) or chief of staff. "I don't have to compromise the secretary's phone if I can get to their EA ... the person who knows what's going on everywhere with everybody." Ramsey added, "Users need to know what to do."

The goal for mobile computing should be "operating in a zero-trust environment," said Matt Scholl, chief of the computer security division of the IT Lab at NIST. "How do you have the technologies that act under the assumption that the ambush is going to happen, that then allows the users in your environment to recover quickly, easily and safely."

Such an environment can provide an antidote to the rising number of phishing attacks, or at least attempts to lure users into clicking on malicious links. In mobile devices, phishing can come both in email (via whichever accounts might be present on a given device) and as text messages. Unlike with regular computers, on mobile devices it's impossible to "mouse over" the link to check its veracity.

Those sending expertly crafted phishing emails, in general, have one of two objectives: planting malware that harvests information off the device or obtaining credentials to gain access to the corporate or agency network.

Bob Stevens, the vice president for public sector at Lookout, calls mobile software the "soft underbelly" of cybersecurity. "The bad guys realize there's a lot of ways to get on a mobile device, and in a lot of cases it's less protected than your traditional desktop or laptop," he said. Most agencies "are starting to realize the mobile device is just another endpoint." But as mobile device management (MDM) gave way to enterprise mobility management and then to mobile application management, a slow procurement process leaves many agencies still in the MDM phase.

Bouquet of Risks

As for the technical risks themselves, Stevens said, "We're starting to see more nation-state activity." For example the ViperRAT surveillance software was aimed at harvesting data from devices of the Israeli Defense Force. It ended up on officers' devices through socially-engineered phishing emails, Stevens said. It harvested photos and contacts, and activated the camera and microphone.

Still another unique mobile threat is the burgeoning population of rogue cell towers from which hackers intercept signals or introduce man-in-the-middle attacks. That's according to Christopher Maynard, acting director of the Office of Chief Information Security Officer at the Homeland Security Department.

NIST's Scholl pointed out the public app stores "are not as clean as they could be." Hiding among the legitimate and vetted apps are some carrying payloads like **ViperRAT**. He recommended using tools available from the Homeland Security Department or from the Defense Information Systems agency for vetting apps.

Scholl said NIST has an active program on mobile security, starting with participation on the security and technical committees of the LTE and 5G standards bodies. He noted it behooves agencies to know what their carriers are doing, because some of the security controls within the LTE standards are optional.

NIST is also continuously touching up its guidance for agencies on MDM, device configurations – and urged security people to look at work being done within the DHS Science and Technology Directorate.

From the carrier perspective, Chris Smith, vice president for shared services at AT&T public sector, noted increasing network virtualization and networks able to tailor data access according to the mission requirements of an agency. He also said agencies have available a wealth of user information generated by behaviors interacting with mobile devices.

"The swipes you do, the apps you access – there's a ton of information. We put this together with this ecosystem of building trust around workloads … to better enable mission delivery," Smith said. Such data can help organizations ensure devices are in the correct users' hands.

Mobile's Many Use Cases

The imperative for mobile security cuts across a wide range of federal missions and use cases.

Maynard at DHS described a focus on multifaceted protection for high-level departmental executives and international travelers. "The focus for us as we're growing the enterprise mobility management picture is on international travelers."

He said DHS uses several technologies, encompassed in an operations security, or opsec, strategy. Opsec focuses on the data and information and looks at it from a vulnerability standpoint. This is combined with making users aware of what to do and not do with their phones. Technical countermeasures include tools that detect the aforementioned rogue cell towers.

For Kenneth Bible, deputy chief information officer at the Marine Corps, the mobile security challenge comes in part from a digitally-native workforce. Sixty two percent of Marines are under 25 years

of age. They do everything on smartphones. That includes operating them in tactical environments with tactical data.

"There's tremendous interest in increasing our use of mobile solution," Bible said. "Our primary focus is supporting the warfighting mission. We have mobile solutions that work in a tactically deployed environment." From a security standpoint, he said the challenge is "how do we separate the data from the device" so the Corps can avoid issuing single-use devices.

Brian Depasse is assistant director for cyber engineering, architecture and identity management at the Justice Department. Mobile computing "is really just a part of everyone's daily work," he said. Whether law enforcement or administrative, employees' use of mobile has spread beyond voice calls and email to encompass core mission functions and activities such as travel and navigation.

Given the ubiquity of smartphones and tablets, AT&T's Smith said security is partly a matter of hygiene. That means keeping software up to date or working carriers to restrict which networks over which agency traffic flows. Beyond that, technologies such as micro-segmentation of data and workloads should be brought more fully to bear on mobile.

Implementation of the domain-based message authentication, reporting and conformance (DMARC) protocols can help the email phishing problems. Agencies are under a DHS binding operational directive to do so. But it won't help with the other vectors into a mobile device. For the time being, only user education and awareness can help with those.

Containerization and micro-virtualization can also help protect enterprise workloads connected to mobile devices, several participants agreed. Tools exist to detect changes in containers and erase them according to preset parameters. Scholl said the SIM card can be used as the reference state for the device and its configuration, against which tools compare the memory banks to discover anomalies.

The initial key to managing and protecting mobile devices, then, is visibility into them. The Marine Corps' Bible added, "The interesting piece is going to be, how does this device management or endpoint management product environment start to converge, include both the traditional desktop and the mobile devices into a single picture."

Tom Temin is a Washington freelance writer with 40 years in business-to-business journalism. E-mail him at tom@tomtemin.com

Lookout

THE SPECTRUM OF MOBILE RISK

Understanding the full range of risks to enterprise data from mobility

Lookout has developed the Mobile Risk Matrix to help organizations understand the components and vectors that make up the spectrum of mobile risk – and to provide data that will help enterprises gain a deeper understanding of the prevalence and impact of mobile threats and vulnerabilities.

THE MOBILE RISK MATRIX

Components of Risk / **Vectors**

	APPS	DEVICE	NETWORK	WEB & CONTENT
THREATS	**App threats** 1 Malicious apps can steal info, damage devices, and give unauthorized remote access.	**Device threats** Device threats can cause catastrophic data loss due to heightened attacker permissions.	**Network threats** 5 Data is at risk of attack via Wi-Fi or cellular network connections	**Web & content threats** Threats include malicious URLs opened from phishing emails or SMS messages.
SOFTWARE VULNERABILITIES	**App vulnerabilities** Even well known software development companies have been found to release apps that contained security flaws, putting corporate and user data at risk.	**Device vulnerabilities** 2 Enterprise devices are at risk during "vulnerability windows," the amount of time it takes from the release of a new patch to adoption of that update.	**Network vulnerabilities** Mobile devices encounter many more hostile networks than laptops, and don't have the same level of protection.	**Web & content vulnerabilities** Malformed content, such as web pages, videos, and photos, can enable unauthorized device access.
BEHAVIOR & CONFIGURATIONS	**App behaviors & configurations** 3 Mobile apps have the potential to leak data such as contact records.	**Device behaviors & configurations** 4 Behaviors like enabling USB debugging for Android or installing apps from non-official app stores put enterprise data at risk.	**Network behaviors & configurations** Connecting to a misconfigured router, unknown captive portal, or a network that decrypts traffic for content filtering.	**Web & content behaviors & configurations** Visiting "low reputation" websites that don't encrypt credentials, leak enterprise data, and increase the likelihood of malicious activity.

MOBILE RISK PREVALENCE

47 IN 1000 ANDROID ENTERPRISE DEVICES ENCOUNTERED APP-BASED THREATS

1 Across two quarters (4Q16-1Q17) 47 out of 1000 Android enterprise devices protected by Lookout Mobile Endpoint Security encountered app-based threats.

57% OF iOS USERS HAVE NOT UPDATED THEIR OPERATING SYSTEMS ABOVE 10.3

2 From the release of iOS 10.3 on March 27, 2017 to April 14, 2017 only 43% of users updated to the latest version of iOS. This is concerning because 10.3.1 patches a code execution flaw that could be exploited via Wi-Fi. This data point is based on iOS users of Lookout Personal.

30% OF APPS ON ENTERPRISE iOS DEVICES ACCESS THE DEVICE'S CONTACTS

3 On enterprise iOS devices protected by Lookout Mobile Endpoint Security, 75% of apps access the camera, 38% access GPS, 8% access calendars, and 10% access the microphone. Across iOS enterprise apps, 43% connected to Facebook and 14% connected to Twitter.

5 IN 1000 ENTERPRISE ANDROID DEVICES ARE ROOTED

4 Only 1 in 1,000 of enterprise iOS devices are jailbroken.

UP TO 1% OF ENTERPRISE MOBILE DEVICES ENCOUNTERED NETWORK-BASED THREATS

5 Lookout research shows that slightly less than 1% of enterprise mobile devices encountered network-based threats over the last year.

ABOUT THE DATA:

The analyzed data came from a large global subset of Lookout personal and enterprise protected devices, and the time periods ranged between April 15, 2016 and April 16, 2017. The enterprise data includes both Android and iOS devices from financial institutions, healthcare organizations, government agencies and other industries. The personal data includes both Android and iOS devices from consumers around the globe, consisting of over 100M devices worldwide. All data was pulled anonymously, and no corporate data, networks, or systems were accessed to perform this analysis.

ABOUT LOOKOUT:

Powered by the largest dataset of mobile code in existence, Lookout is the security platform of record for mobile device integrity and data access. Lookout is trusted by more than 100 million individuals, hundreds of enterprises, and government agencies, and ecosystem partners such as AT&T, Deutsche Telekom, Microsoft, and Verizon. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto, and Washington, D.C.