Keeping the public sector safe in the mobile age

AS MOBILE USE RISES, SO DO THE RISKS

White Paper | March 24, 2020

Written by: Elizabeth Lindsay – Advanced Cyber Security Inc. – Strategic Advisor and Partner to Cromtec Cyber Solutions.

CROMTEC CYBER SOLUTIONS
PROTECTING YOUR MOST VALUABLE DIGITAL ASSETS!

ACS
Advanced Cyber Security Corp.

In 2016, mobile traffic surpassed desktop for the first time, and by 2018, 70% of all internet traffic came from a mobile device.[1] Today, 81% of Americans own a smart phone, 76% open and respond to emails on their mobile device, 79% use their mobile device to make online purchases and 76% check their banking balance using mobile. [2] [3] [4] [5] Retailers, banks and organizations of all kinds have quickly come to realize that having a mobile app helps retain and obtain more customers and members. In fact, 90% of the U.S. population's mobile time is spent using apps.[6] As of the fourth quarter of 2019, there were 2.57 million apps in the Google Play store and 1.84 million in Apple's App store. [7]

CYBERCRIMINALS TURN THEIR ATTENTION TO MOBILE

In this increasingly mobile world, cybercriminals have turned their attention towards smartphones, which represent a vast opportunity for financial gain. Today, people hold more information on their smartphones than they do in their home. For this reason, a study conducted in March 2019, found that the number of attacks using malicious mobile software has nearly doubled from the previous year. [8]

HOW DIGITAL TRANFORMATION AND THE INCREASE IN MOBILE USAGE IMPACT THE PUBLIC SECTOR

From federal agencies (whether civilian agencies or defense and intelligence agencies) to state and local governments, organizations in the public sector are advancing digital transformation with an emphasis on mobile to better serve constituents, protect the homeland, connect citizens with data and increase agency efficiency. Through all this change, government IT and security professionals are challenged to protect sensitive government and citizen data, while remaining open and transparent to stakeholders. As agencies and their partners work to make government more accessible to citizens through online and

mobile experiences, there is always a risk that these activities will also make operations and data more vulnerable to cyberattacks.

While no organization is immune to a data breach, the public sector is particularly vulnerable. In recent years, attacks on non-profits, government agencies and other institutions within the public sector have skyrocketed. Of all industries and sectors, government/military are among the highest rate of data breaches. In 2018 alone, there were 100 government data breaches which involved 81,505,426 stolen records. Within the last 6 years, the U.S. Postal Service / Office of Personnel Management (OPM) has been breached twice exposing a total of 63,650,000 records. [9]

PUTTING CITIZENS AT RISK

Government agencies are targeted for their wealth of personal information on citizens. Agencies such as the IRS house social security numbers, addresses, work history, banking information, email addresses and more. In addition to the types of personal details the government collects, the sheer volume of records is staggering. This information is valuable to criminals, especially foreign governments in which acquiring sensitive data about U.S. citizens and uncovering government secrets is part of their mission. Government records can be exploited in many ways, including tax fraud. In addition to filing fraudulent tax returns, criminals can use a victim's personal details to receive government benefits, apply for a job, and gain restricted clearance. To address these tax scams, the IRS now features Identity Theft tips and resources on their website to help victims. [10]

STUDENT MOBILE DEVICES: AN EASY TARGET

According to a recent study conducted by the Federal Trade Commission (FTC), college age students are the most frequent victims of ID theft. [11] Experts believe it may be because they are young and inexperienced in cyber safety, spend more time on their mobile device than any other demographic, they are much more

likely to share personal information and they typically don't check their credit reports. Every day, students expose their identity when they routinely type in their personal information into online order forms, banks, social media and more. As a student enters college, they are consistently asked for their social security number for offers from credit card companies, new doctors, student loan forms and more. In fact, reports of student loan fraud surged more than 120 percent from last year. Students aren't the only ones exposing their identity. Each year, universities report data breaches that expose thousands of student personal records. Academic networks contain a wealth of student data including full name, social security number, birthdate, home address and payment information. This kind of data is a big payday to hackers. [12]

PHISHING AND SMISHING

Hackers are delivering their mobile malware to both citizens and organizations in a number of ways. Phishing and SMSishing are methods used to trick victims into clicking on infected links inside email and mobile text messages. This often leads to the download of malicious software. In September, 2019, the IRS put out a statement warning tax professionals of phishing email scams and malicious software called keyloggers that log every keystroke and are used to steal taxpayer's data. [13] In even more recent news, researchers found that hackers are using the current Coronavirus fears to trick victims into new online scams that steal personal and financial information. Some cybercriminals are using the logo of the WHO (World Health Organization) to spoof official advice emails, which trick users into downloading the keylogging malware named AgentTesla, potentially giving hackers access to online banking accounts and other sensitive data. [14]

FAKE APPS

According to McAfee's 2019 Mobile Threat Report, "Fake apps have also become a rampant problem for Android and iPhone users alike. This is mainly in part due to

malicious apps hiding in plain sight on legitimate sources, such as the Google Play Store and Apple's App Store." Fake mobile apps are Android or iOS applications that have copied the look and/or functionality of legitimate applications and are used to trick unsuspecting users to install them. Once downloaded and installed, the applications perform a variety of malicious actions. Some fake applications are designed to harvest credentials, intercept sensitive data, divert revenue or infect devices with malware that puts all data typed into a device at risk of being stolen. In November, 2019, counterfeit apps were found carrying a new version of the Android banking trojan called Ginp that has the capability to trick the victim into stealing user login credentials and credit card details." [15] According to the McAfee 2019 report, Nearly 65,000 new fake apps were detected in December of last year alone— over 6 times the amount reported in June 2018." [16]

REFERENCES:

1. https://www.ciodive.com/news/70-of-internet-traffic-comes-from-mobile-phones/510120/
2. https://www.pewresearch.org/internet/fact-sheet/mobile/
3. https://hostingtribunal.com/blog/mobile-percentage-of-traffic/#gref
4. https://www.outerboxdesign.com/web-design-articles/mobile-ecommerce-statistics
5. https://thefinancialbrand.com/73785/banking-digital-payments-ing-paypal-credit-debit-cards-p2p-trends/
6. https://hostingtribunal.com/blog/mobile-percentage-of-traffic/#gref
7. https://www.statista.com/statistics/276623/number-of-apps-available-in-leadingapp-stores/
8. https://www.techradar.com/news/mobile-malware-attacks-double-in-2018
9. https://news.clearancejobs.com/2019/07/26/top-government-data-breaches/
10. https://www.irs.gov/identity-theft-fraud-scams/identity-protection-tips
11. https://www.ftc.gov/news-events/blogs/business-blog/2019/02/top-frauds-2018
12. https://www.cnbc.com/2019/08/29/hackers-are-targeting-colleges-for-students-data.html
13. https://www.irs.gov/newsroom/heres-what-tax-pros-can-do-so-they-arent-taken-on-a-phishing-trip
14. https://www.techradar.com/uk/news/coronavirus-malware-scams-return-with-a-venegeance
15. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ginp-trojan-targets-android-banking-app-users-steals-login-credentials-and-credit-card-details
16. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf