Lookout

Whitepaper

Predictive Security

Using big data to unmask mobile threats

Written by Aaron Cockerill, VP of Products, Lookout

I. Introduction

Don't worry, guys. Mobile threats for enterprises don't actually exist, so we can put off figuring out how to protect them for a little while longer. After all, major corporate breaches like J.P. Morgan, Target, and Sony are coming from other attack vectors, right?

The reality is, many of the big corporate breaches we hear about in the news are coming from a number of threat vectors. Sony was allegedly hacked through PCs, Target through point of sale systems, J.P. Morgan likely through unprotected server infrastructure. Mobile is just another one of these vectors and, believe it or not, corporate-concerning mobile threats already exist. The way we protect our devices should be top-of-mind and is clearly in for a major overhaul.

I happen to think the answer to that "major overhaul" is big data and the machine intelligence tools that make sense of it all.

II. Mobile threats are a "when" not "if" problem

Mobile malware that faces the enterprise is on the cusp of some major change. NSA director Michael Rogers spoke in November on securing U.S. infrastructure calling mobile threats a "coming trend" and that government officials are worried about mobile attacks against government and corporate networks. Indeed, a recent study from BT states that mobile breaches affected 68% of global organisations in the last 12 months. I can think of a few threats that corporate networks should be paying attention to now: Wirelurker, XAgent, and NotCompatible.

III. What's wrong with the way we protect our systems now?

That all sounds pretty bad, but believe it or not, we're not losing the war, we're just using the wrong defenses. Right now we have two tenants of security that have lived long past their use-by dates as individual models of security: signature-based and behavioural-based detection. We actually need both of these security models to work together in combination with a third: predictive security.

Standalone signature-based security is antiquated. Malware authors have long-since learned that if you change a very small piece of your malicious app's code you'll be able to trick anti-virus detection that relies on signatures.

Behavioural-based security is better, but also not enough on its own. It's like putting code into an isolated environment and then, effectively, poking it with sticks to see what it does. If it does nothing it's safe, right? Wrong. Malware authors innovate and have developed ways to hold back their malicious behaviour while living in these virtual behavioural detection systems and begin exhibiting bad behaviour only once the coast is clear. Behavioural analysis only catches lazy malware developers.

IV. So, what's this predictive bit?

Here's where big data comes into play. To be predictive you need to have insight into the whole world's mobile code. Predictive security takes into account both signature- and behavioural-based security, but adds in a layer of data and machine intelligence. It knows what bad code and bad behaviour look like and then matches that data to potentially bad apps so that an attack can be stopped before any harm is done.

Without this data -- or the machine intelligence used to process it -- security technology will never mature to the point where it can predict when an app is about to go bad.

Take, for example, a bad app called MalApp.D. The app which was masquerading as a common VoIP app in the Google Play store, was actually connected to a crime ring otherwise associated with malicious banking malware. While it would seem normal for a VoiP app to access contacts and other communications-related data, the app was actually set up to send this information back to a malicious command and control server.

Through multidimensional correlation, predictive security revealed that this VoIP app was, with an extremely high likelihood, developed by a known malicious group.

Another threat, called BadNews, gives another great example of predictive security in action. The malware lived inside of a number of applications found in the Google Play store. Positioned as an advertising network, it used technology to hide its bad behaviors while going through Google's app-vetting system Bouncer. Once on the device, however, BadNews was able to push fake news prompts to users and install further malware. Using code similarity, predictive security was able to determine that this code was bad and stop it.

Of course, when you're talking about big data, you need to consider the scale at which new data is created. App stores today are publishing tens of thousands of new apps or updates to existing apps all of which need analysis. It's going to take automated machine intelligence systems as a key element of predictive security to handle the load.

V. So, what now?

The enterprise needs to understand the costs and benefits associated with predictive security. At its core, it's coming to appraise the value of the data your corporation hold. Some of this is obvious: proprietary technology plans saved in cloud storage or financial information. Some of it is less obvious, however, such as contact information. If you're an intern, the contacts on your device aren't likely all that important, but the vice president of sales for a defense contractor might have some contact information for some intriguing people a bad guy might like to learn more about.

You've got to get in the bad guy's head when considering this, realising that predictive security is doing the same.

This reactionary security landscape is not working. We need get ahead of the curve. It's time for corporations to start asking their security vendors how they predict threats.