Mobile Threats | MalApp

HOW LOOKOUT'S PREDICTIVE SECURITY UNMASKED A MOBILE THREAT

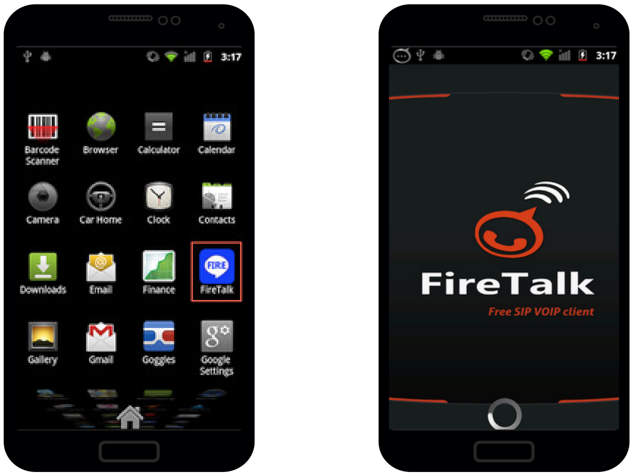
Introduction

To detect advanced threats that can evade signatures and behavioral analyses, Lookout developed a platform that provides predictive security. The Lookout Security Platform collects a massive dataset of the world's mobile code and uses correlations and machine intelligence to detect threats without signatures and can detect threats before they exhibit malicious behavior by revealing their "genetic relation" to bad actors and code. The power of this approach is evident in Lookout's recent detection of MalApp.D, a mobile threat that matched no prior signature nor engaged in overtly malicious behavior, but nonetheless put enterprise contact data and communications at risk.

MalApp.D was embedded in a seemingly benign VoIP app called FireTalk that was actually live in the Google Play Store at the time of Lookout's detection. Through multidimensional correlation Lookout's platform revealed that this VoIP app was, with an extremely high likelihood, developed by a known author of mobile malware and given its access to device contacts and potential call recording capabilities it posed an unacceptable risk to enterprises.

Unmasking MalApp.D

MalApp.D hid in plain sight, disguised as a VoIP app called FireTalk, which had only been live in the Google Play Store for 48 hours at the time of Lookout's predictive detection:



Screenshot of MalApp.D (FireTalk) icon and splash screen.

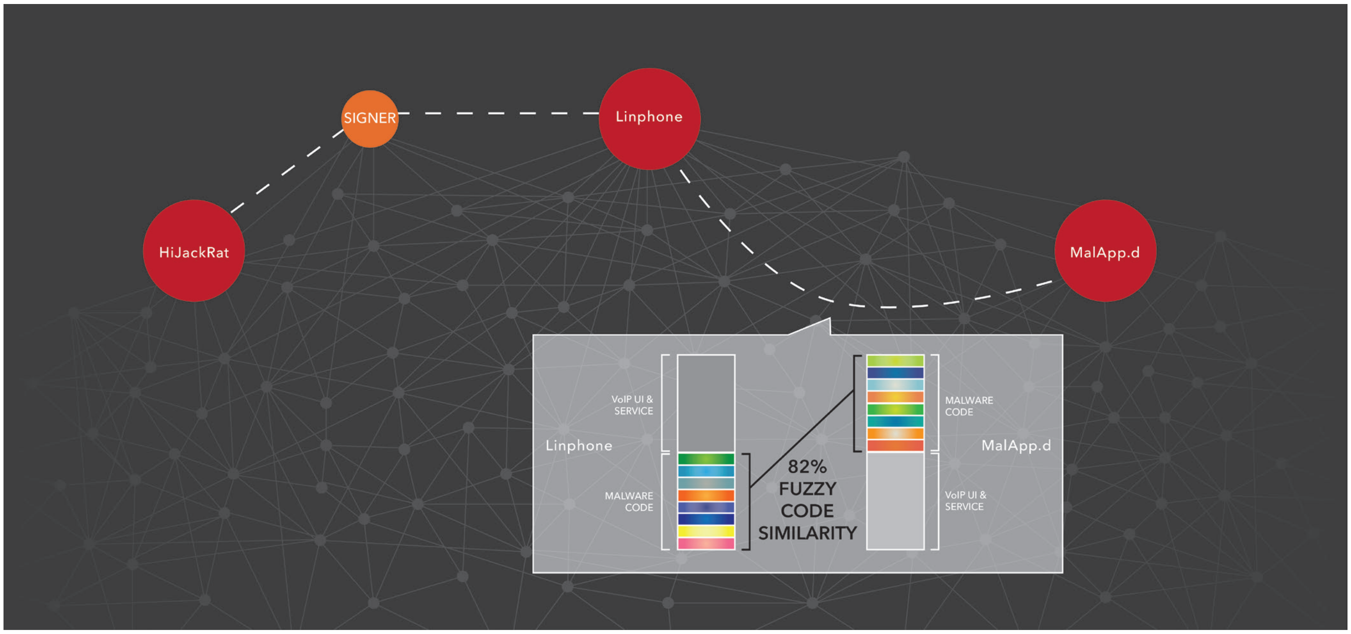
With a handful of positive reviews and a 4.2 star rating in the Play Store, FireTalk (MalApp.D) appeared legitimate. The app requested permission to access device contacts, a common request among communication apps who often need this data to facilitate their functionality.

Running FireTalk in a behavioral analysis sandbox revealed that it also copied these contacts over to a server, which, while a potentially risky behavior, does not automatically signal maliciousness as this behavior is not uncommon amongst legitimate apps. Historically, given the lack of a signature and overtly malicious behavior, a threat like FireTalk (MalApp.D) would go undetected indefinitely or until the app was determined to be part of the kill chain during a post-mortem breach investigation.

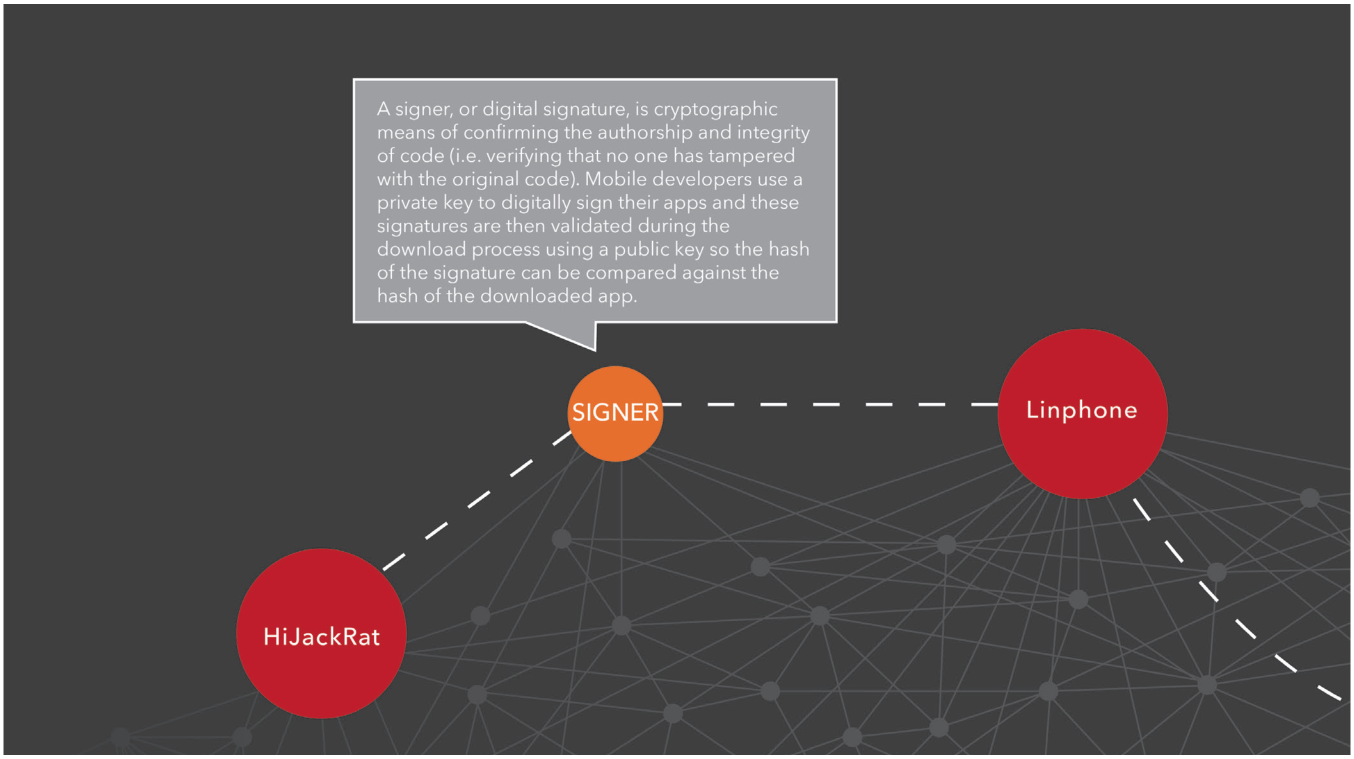
Predictive security, however, offers an alternative. In this case, two core components of Lookout's predictive approach, App Genome Sequencing and multidimensional threat correlation, helped identify this app as highly risky.

The detection of FireTalk (MalApp.D) would not have been possible without Lookout's mobile intelligence dataset, which contains hundreds of millions of data points on more than six million mobile applications. This dataset contains a malware family found outside the Google Play Store called HiJackRat, which has historically engaged in banking fraud in Korea by posing as a legitimate banking app and capturing victims' login credentials.

Using multidimensional threat correlation, Lookout first detected that a newly acquired app, a Chinese VoIP app called LinPhone (also a non Play Store app), used the same private key to sign the app as a sample of the HiJackRat family. LinPhone, however, had distinct code and functionality and was not a member of the HiJackRat family.

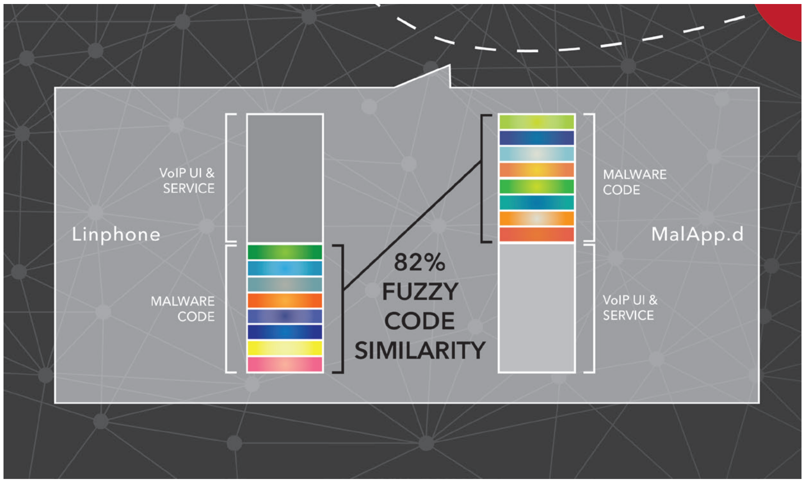


A diagram showing Lookout's detection of MalApp.d


A signer, or digital signature, is cryptographic means of confirming the authorship and integrity of code (i.e. verifying that no one has tampered with the original code). Mobile developers use a private key to digitally sign their apps and these signatures are then validated during the download process using a public key so the hash of the signature can be compared against the hash of the downloaded app.
SIGNER
Linphone
HiJackRat

LinPhone shared a signer with a sample of the HijackRat family.

When Lookout later acquired FireTalk from the Google Play Store, the Lookout Security Platform identified a high degree of code similarity between FireTalk and LinPhone using App Genome Sequencing. Code similarity in this case does not mean simple 1:1 string matching; rather, App Genome Sequencing is an automated process of fuzzy code matching that compares app code blocks and assesses their holistic similarity, with percentage outputs not unlike a genetic test. In the case of FireTalk and LinPhone, the malicious blocks of analyzed code were found to be more than 82% similar, indicating unmistakable relation between the two and evidence of their membership in a new malware family, MalApp.D.



App Genome Sequencing reveals code similarity between LinPhone and MalApp.d.

The predictive security capabilities of Lookout's platform identified FireTalk (MalApp.D) as a threat through its relation to known bad actors. It's not the de facto capabilities or behavior of FireTalk that make it a threat, it's the context of those capabilities in the hands of malicious actors that makes it an app no enterprise would want an employee to have installed on their device.

Predictive security technology only works if it has global context. The continued failure of anomaly detection and behavioral analysis alone to reliably identify threats without oceans of false positive results demonstrates the importance of having large, contextual datasets. Lookout's platform excels at finding the signal amid the noise because it has insight into what code is running on tens of millions of mobile devices around the planet, and leverages a dataset of more than six million unique app binaries containing hundreds of millions of potential threat indicators.

Understanding the Enterprise Risk

The capabilities of FireTalk (MalApp.D) are especially concerning in an enterprise environment:

EXFILTRATION OF DEVICE CONTACTS

In corporate environments with contact data sensitivity, this capability of FireTalk (MalApp.D) in the hands of a malicious actor could be used to gather reconnaissance for a spear phishing attack against enterprise systems.

POTENTIAL CALL RECORDING CAPABILITIES

Like all VoIP apps, Firetalk (MalApp.D) talks to a server through which it routes communications, raising the possibility that in the hands of a malicious actor it could be used as a means for wiretapping corporate conversations. VoIP apps (like FireTalk) use Session Initiation Protocol (SIP) and in theory could record these conversation on the server-side. This would make it relatively easy for attackers to capture communications without raising victim suspicions due to excessive battery or bandwidth consumption.

Conclusion

Not only did MalApp.D sneak past Google, but Lookout was also the first and only security vendor to detect it (within 48 hours of it being live in the Play Store) and Lookout immediately pushed protection to its users while notifying Google (who subsequently removed it). The detection of FireTalk (MalApp.D) is a strong validation of Lookout's predictive security platform, since approaches that depend on signatures or behavioral analyses alone would likely never have detected it.

The power of predictive security lies in its ability to draw insights from an enormous global dataset and identify complex threat correlations that exceed human analytical capabilities. Lookout's App Genome Sequencing technology, for example, breaks an application into code markers and automatically correlates them against hundreds of millions of markers from apps around the world. To avoid App Genome Sequencing, attackers would need to rewrite their entire codebase, a cost prohibitive obstacle compared to the relatively simple modifications needed to evade static signatures and behavioral analysis technologies.

Predictive security is only as effective as the comprehensiveness of the dataset on which it depends. In this case, for example, neither LinPhone nor HiJackRat were found in the Google Play Store so the correlations between these threats that later enabled the identification of FireTalk as a threat would not have been possible were it not for the comprehensive reach of Lookout's platform. Lookout's global sensor network of more than 50 million devices combined with its security partnerships with some of the world's largest app stores means the Lookout Security Platform collects application binaries that no other security vendor will ever see, including hundreds of thousands of apps that have only ever existed on a single device in the entire world. The scale of Lookout's dataset, paired with cutting edge machine intelligence enables Lookout to proactively detect MalApp.D and its ilk while keeping both consumers and enterprises safe. ■