Briefing Note

Machine Learning: a New Frontier in Mobile Phishing Protection

Introduction

Mobile devices today are particularly susceptible to cyber attacks as more and more companies evolve into a 'mobile workforce'. Employees that use mobile devices for both personal and professional business receive communications through an increasing number of channels, meaning that instead of just email, organizations are now exposed to phishing attacks through platforms such as SMS, messaging services like WhatsApp and Facebook Messenger, and social media sites like Twitter, Facebook and Instagram. As well as this, employees are constantly on the move, connecting to countless Wi-Fi and mobile networks and without the protection of the corporate network, are left exposed and vulnerable to threats. Cyber criminals are aware of all of these factors and as a result are constantly trying to exploit mobile users with phishing sites, malware downloads and social engineering attacks. As well as this, the current cyber threat landscape is constantly changing and evolving in response to developments in technology and as a result, it can be difficult to anticipate and protect from potential threats.

'Zero-day' attacks

One of the most concerning examples of this constant attempt at attack is the development of 'zero-day' phishing attacks. Due to the real-time, constantly-connected nature of mobile, phishing attacks continuously develop and evolve and today, most phishing campaigns are created, deployed, engaged and dissolved all in a time frame as short as a single day. By publishing phishing sites online for such a short period of time before moving to an entirely new hosting server, hackers can easily evade detection while users are left with hardly enough time to identify, let alone prevent, the attack from occurring. Businesses and individual users must be constantly aware of new emerging risks and attacks, however with over 46,000 new phishing sites created per day, with the majority of these online and active for only 4 to 8 hours, this is simply impossible.

Where this human knowledge fails, users usually rely on anti-phishing and cyber security solutions to detect and protect from attacks, however in the case of these 'zero-day' campaigns, often the threat has done its damage and moved on before it can be detected or logged to a database, rendering the security software useless. It is in these initial few hours, before threat intelligence feeds can be updated, that users are most at risk and mobile devices are most

vulnerable.

Mobile Machine Learning

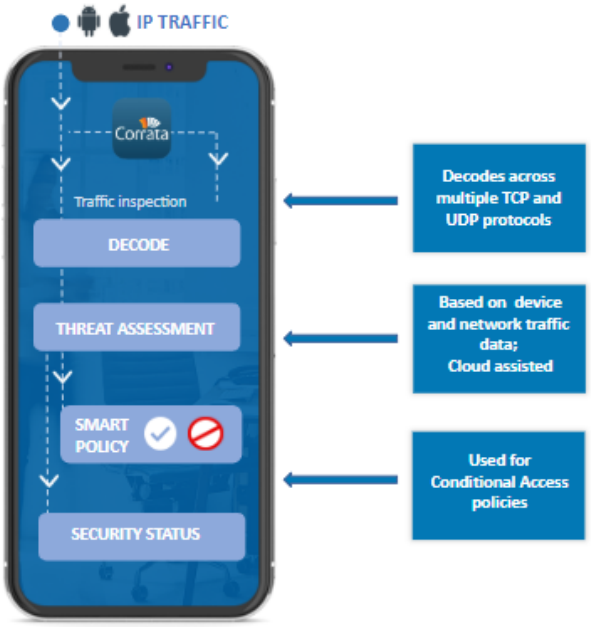
A major breakthrough in this attempt to anticipate and prevent cyber-attacks is the development of mobile Machine Learning solutions. Cutting-edge Artificial Intelligence (AI) technologies have made it possible to detect and react to threats as they are created, meaning users no longer have to rely solely on lists of known malicious sites in order to prevent malware infection or phishing attacks.

Machine Learning (ML) is a branch of AI based on the concept that systems can learn from data, identify patterns, and make decisions with minimal human intervention. It is becoming a key aspect of cyber security and will likely have a major effect on the fight against cyber-crime. The idea that computers can learn from previous computations and results to produce reliable and repeatable decisions is not recent, however growing volumes of available data and powerful developments in computational processing have led to a resurgence and growth in the process. The use of machine learning has already been deployed in various different forms, from Google's self-driving cars to Netflix's movie-suggestion algorithm, but as technology continues to develop to produce models that can analyze bigger, more complex data and deliver faster, more accurate results even on a very large scale, it is clear that Machine Learning is fast becoming the new frontier in digital service delivery and has especially become a major factor in the area of cyber-security.

Corrata's SafePathML solution

In response to 'zero-day' phishing attacks, Corrata have developed a cutting-edge mobile Machine Learning security solution that can preemptively detect and block phishing attacks as they are created. Corrata has identified a range of parameters which can act as indicators of unsafe domains. Using our dataset of malicious and safe domains, we continuously train our SafePathML algorithm to accurately assess the probability of a domain being unsafe, allowing us to block threats even before they have been identified by the wider cyber-security community.

Machine Learning is based on continuous learning and the Corrata solution is constantly improving. As the model successfully identifies phishing attacks and malicious sites, it is refining its accuracy and ability to recognize the parameters of unsafe domains and is therefore constantly increasing its reliability to protect mobile devices from 'zero-day' threats. By working with existing threat intelligence databases, Corrata's SafePathML solution ensures that employee devices are always protected from all phishing or malicious cyber attacks, regardless of when they are created or where they are hosted.



Want to find out more about machine learning and how it can provide robust protection from zero-day threats?
Contact Corrata today