corrata

Technical Brief

3 Key Developments in Mobile Phishing That Every Organization Should Know

Introduction

Internet phishing is not a new threat. It has existed for many years in many different forms, constantly evolving and becoming more sophisticated in response to technical trends. Because of this, however, it is essential that organizations and their phishing detection and protection solutions are also able to adapt in response to changes. Recently Cofense (the company formerly known as PhishMe) and Proofpoint published their annual phishing reports. Cofense's 'The State of Phishing Defense' and Proofpoint's 'State of the Phish' are widely regarded as authoritative sources on the current trends in both phishing campaigns and the capabilities of organizations to defend against such attacks. Not surprisingly, mobile features prominently in both reports and below we outline three key takeaways from the reports as they relate to mobile phishing.

1. Look beyond email

One of the main points outlined in Cofense's report is that sensible risk management means a company should know where its vital assets are, and which types of attacks pose the greatest threats. In short, protection efforts should be focused on what matters most to the business. Today, with smartphones and tablets now accounting for over 60% of all smart connected consumer devices it is clear that focus should be shifting towards mobile. While email remains the easiest and most frequent attack vector, other social engineering techniques specific to mobile, are beginning to increase rapidly in their use for phishing attacks and should not be ignored. The 2018 Proofpoint User Risk Report found that 90% of 6000 working adults surveyed had a smartphone, with 39% using these devices for a blend of work and personal activities. With more employees accessing corporate data via mobile devices and many cybercriminals using methods such as pretexting, vishing (voice phishing), and smishing (SMS phishing) to penetrate organizational defences, it is clear that security focus also needs to shift towards mobile.

At Corrata we understand that mobile devices, such as smartphones and tablets, have become essential to our everyday lives both at work and at home. While their increased use for work has allowed employees more convenience and flexibility for greater innovation and productivity, new avenues for cyberattacks have also emerged. As well as methods like 'smishing and vishing as outlined by Cofense, we have also seen a rise in phishing attacks using online messaging services such as WhatsApp, social media sites like Facebook and Instagram, and apps downloaded to the device from both official and unofficial app stores. In response to this, Corrata was developed specifically to extend the security usually afforded to desktops to mobile devices. Our Security and Control solution detects and prevents access to phishing attacks on every platform, including email and mobile-specific vectors, to ensure organizations are fully protected where it matters most as enterprise mobility continues to grow.

2. Attacks constantly evolving

One of the greatest difficulties posed by phishing threats today is their ability to quickly adapt in response to changes in technology and cybersecurity solutions. Due to the real-time, constantly-connected nature of mobile, phishing campaigns are continuously evolving with most attacks created, deployed, engaged, and dissolved all in a time frame as short as a single day. Businesses and internet users must be constantly aware of new emerging 'Zero Day' attacks, but with over 46,000 new phishing sites created per day, and the majority online and active for little more than 4 to 8 hours, this is becoming more and more difficult.

Where human knowledge fails, users usually rely on anti-phishing and other cyber-security software to detect and protect from attacks, however the shortcomings of their 'known bad' approach is highlighted in Cofense's report. Security solutions designed to fight existing or known threats create gaps in the cybersecurity landscape that hackers are happy to exploit. By publishing phishing sites online for such short periods of time before moving to entirely new hosting servers, the threat can do its damage and move on before it can even be detected, rendering the security software essentially useless. It is in these initial few hours, before threat intelligence feeds can be updated, that mobile devices are most vulnerable and security solutions are most needed to detect and respond to threats.

A major breakthrough in the attempt to anticipate and detect Zero Day phishing attacks in real-time is the development of machine learning solutions based on constant improvement. Solutions like Corrata's SafePathML use continuous learning from datasets of malicious and safe domains to accurately assess their legitimacy and detect threats even before they have been identified by the wider cyber-security community. Working with existing intelligence databases while also detecting these Zero Day attacks ensures that mobile devices are protected from all phishing attacks, regardless of when they are created or how they evolve.

3. Visibility is crucial

You cannot defend against attacks you cannot see. One of the main messages highlighted in Cofense's report is that visibility is core to any security operation and that an attack cannot be mitigated if the organization has no knowledge of its existence. A lack of comprehensive visibility, increased layers of technology, and poor employee awareness can often create a fog that obscures the threat of phishing attacks. In their 2019 Report, Proofpoint found that many employees lacked an understanding of basic cybersecurity terms, especially those specifically associated with mobile, and were therefore unable to actively defend themselves from attack.

For example, 66% of respondents were correctly able to describe 'phishing' however, only 23% were able to explain 'smishing' and only 18% could correctly describe 'vishing'. End users play a significant role in the battle against phishing by recognizing and identifying threats as they arise, however this cannot be expected without effective security awareness training.

Visibility is also a crucial element in anti-phishing software solutions. This is one of the main elements of Corrata's Security and Control solution which, unlike other solutions, probes deeper to see the metadata associated with all device network activity across multiple layers and protocols such as Wi-Fi, cellular, IP, TCP, and HTTP. This granular level of visibility means we analyze 1000's of discrete data points per device per day, allowing us to see and respond in real time to even the latest phishing attacks.

Key Takeaway

With phishing quickly becoming one of the most prevalent cyber threats facing modern organizations, and with reports such as these from Cofense and Proofpoint, it is clear that the ability to evolve to detect and protect from attacks as they occur is quickly becoming one of the most essential aspects of organizational security. And with mobile usage growing so rapidly in enterprise, it is no surprise that the methods used by phishing attacks have evolved to focus on mobile-based platforms, leaving security and defense solutions with no other option but to follow suit.

Want to find out more about mobile phishing and how to ensure your devices are protected?

Contact Corrata today