ADDRESSING NEW MOBILE THREATS WITH CLIENT-SIDE BROWSER ISOLATION SOLUTIONS

Along with the growth and popularity of mobile applications and mobile web comes a surge of attacks on mobile devices. According to several studies, mobile operating systems and browsers lack secure application identity indicators, leading to users not knowing where links have taken them, which is exacerbated by the growing linking between websites, mobile applications, and cloud-based services including productivity and collaboration enterprise applications.

Users are regularly asked to provide their usernames and passwords, which can be a gold mine for cybercriminals, given how vulnerable content applications are to spoofing. As millions of workers were forced to work remotely given the global healthcare crisis in 2020, the world saw an unprecedented number of cyberattacks when legitimate applications were spoofed with high accuracy.

In this white paper you will learn more about these threats and how client-side advanced web and threat protection technologies work in our increasingly decentralized world.

INTRODUCTION

Consider the size of a smartphone screen compared to a large desktop computer monitor – while being able to access nearly everything now on a smartphone or tablet is extremely convenient, the smaller the screen, the more difficult it may be for a user to identify a malicious versus official application.

For example, a user may be doing research, looking at an article published about a new streaming service, and may click on an embedded link that indicates the user will be taken to the streaming service website to sign up for a free month. Little does that user know they have gone to a malicious site which asks for personal information, authentication credentials, credit card or other payment information.

The user, an employee of large bank, has just opened the door to their mobile device and cloud services subscriptions simply by making a bad decision given how realistic this imposter experience was. The lack of secure identity indicators made this possible, and it could be hours or days, even weeks or months before the user would be able to tell they had been sent to the wrong target.

In a direct phishing attack, the sender is a malicious application that links the user to its own spoof screen instead of the real target application.

On the other hand, in a “man-in-the-middle” attack, the sender is benign, but another party intercepts the link and loads a spoofed target application in place of the intended target application.

Android and iOS systems and browsers use simplistic interfaces to ensure readability, and it is precisely this simple approach that makes it easy for cybercriminals to mimic legitimate sites. Additionally, unlike a “fixed” browsing experience, only one screen can be seen at a time, and that screen does not show the identity of the application in the same way as it is shown on a laptop or desktop.

On the other hand, in a “man-in-the-middle” attack, the sender is benign, but another party intercepts the link and loads a spoofed target application in place of the intended target application.

Android and iOS systems and browsers use simplistic interfaces to ensure readability, and it is precisely this simple approach that makes it easy for cybercriminals to mimic legitimate sites. Additionally, unlike a “fixed” browsing experience, only one screen can be seen at a time, and that screen does not show the identity of the application in the same way as it is shown on a laptop or desktop.

Mobile browsers display only one browser window at a time and most web sites hide the URL bar once the page has loaded. If a user wants to see the URL bar, the user can tap the top of the screen, which is not typically done according to many UX research studies.

Mobile applications are less trusted than their desktop counterparts. In Android and iOS, applications are isolated from each other by default; for example, applications cannot read each other’s databases or network traffic. Additionally, Google and Apple attempt to prevent users from installing malware by controlling how users install applications.

Application permissions are supported by Android and Apple operating systems, controlling access to privacy and security settings, and users can decide which permissions to grant (for example location, contacts, etc.) informing users of the risks of installing applications. Listing applications in the app stores brings with it security standards and testing, and while specific details the review processes are considered secret, the process includes a security review.

But this applies only to mobile apps. Apple and Google review the applications that are going to be put on their application stores and blocks them if they find any malicious activity – however they don't restrict web browsing.

ADDRESSING THE CHALLENGES OF MOBILE BROWSING

Mobile applications (except financial applications) commonly store their users' passwords so that users will not need to re-enter them. Users must, however, enter their passwords into the web versions of these applications, either in the browser or as embedded web content. Users instinctively enter passwords when they see an appropriate login screen for a mobile target.

Control transfer happens when the user clicks to a new mobile web page, and stops interacting with the previous application, and starts interacting with the new one. This can happen from one web experience to another, from an application to a website (based on the embedded link), or from a web experience to a mobile application. It has become increasingly easy to embed links and APIs, and the web browsing experience is becoming exponentially faster and more appealing with 5G speeds being rolled out – which will only exacerbate the risks.

Sharing has become extremely popular on social media, and delivers "instant gratification" – for example, a seemingly legitimate web site or link on a mobile user's screen may be tempting to post on Facebook, where followers can be attracting to also click on what could be a malicious site, and even share that forward, leading to "viral phishing" opportunities for sophisticated cyber rings.

Another notorious honey pot is associated with "free trials" – users get 30 days to try a service, but they must put in their details, including payment methods, in advance – to continue service, or continue service without advertisements. Upgrades. Developers sometimes publish two versions of an application: a free version with limited functionality or banner advertisements, and a paid version with full functionality or no advertisements.

While most of these situations are legitimate, they have conditioned users to input private and sensitive information, including passwords that may be risky if used across many applications. Free applications drive adoption orders of magnitude faster than those requiring paying in advance, so are popular with developers, and users have simply gotten into the habit of trusting the process.

Enterprise cybersecurity teams can provide training and offer reminders of all these risks through some products that look and remove malicious apps installed on the mobile phone , but ultimately given the pace of business and the new way of remote working, to reach a "zero-trust" goal, advanced web and threat protection technologies make it possible for users to go with the flow throughout the day, while on their mobile devices, with the automatic support of software embedded on their device that warns about risky web sites or mobile apps before they engage, or disallows those domains altogether.

TYPES OF MOBILE PHISHING ATTACKS

As the number of phishing attacks grow, and the severity of the attacks broaden, those initiating attacks are using increasingly sophisticated methods to lure end-users to engage. The three main categories are:

FAKE BROWSERS

Fake browsers look like Chrome, Firefox, Edge, Safari and others and trick end-users into clicking to learn more. The infection chain starts with a legitimate website injected code from a file sent by of its URLs. The injected code is highly-obfuscated, however the URL most often ends with a .js. Hackers often use “update your software” approaches, including using email links or script code to compromise a webpage. The code results in a message box popping up that tells users a critical error happened due to using an outdated web browser, as one scenario.

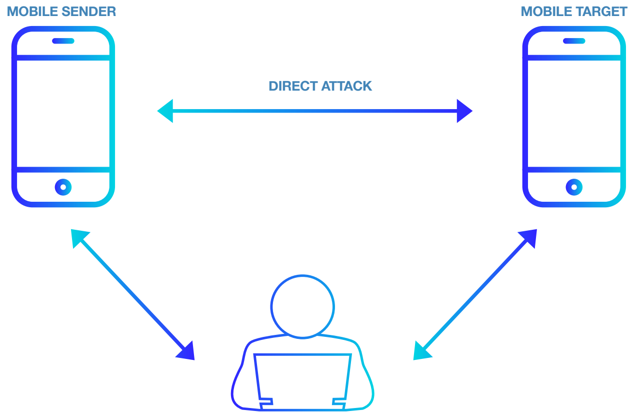
EMBEDDED WEB CONTENT

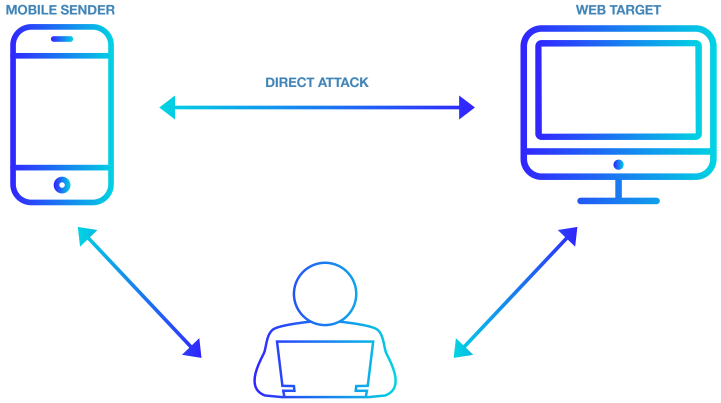
Embedded web content phishing schemes use links contained in text or an image that lead to another page on the web when clicked. Attackers with malicious intent hope users click an embedded link (often in an unsolicited email or message) that will take them to a fake but realistic looking website. When the visitor goes to the website, there may be a variety of phishing tactics designed to exploit users, for example collecting personal information provided on the site or initiatiating code that silently downloads malware.

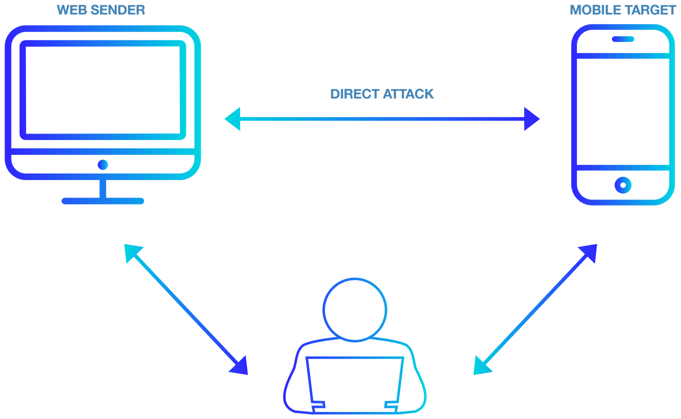
SPOOFED WEB SITES

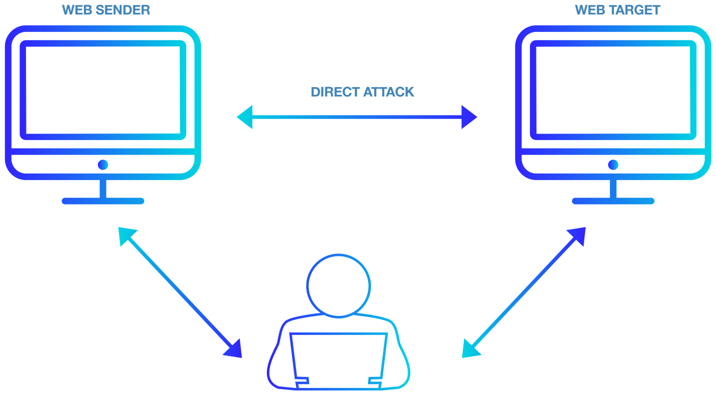
Spoofed websites mimic legitimate websites with the intent to build trust and get end-users to interact. The most successful spoof websites adopt the exact design of the real website, and come with a similar URL. Sophisticated attacks include the creation of a "shadow copy" of the World Wide Web, and once the end-user has engaged, all their traffic goes through the attacker's machine where sensitive information can be picked up. A third example is using domain forwarding, inserting control characters so the URL appears to be genuine while concealing the actual address of the malicious website.

With the popularity of mobile browsing, online collaboration and communication, and the constant use of mobile devices with small sreens, these three types of attacks trick mobile users often faster than they would if the same user is concentrating at their desk, and viewing a larger screen


MOBILE SENDER
DIRECT ATTACK
MOBILE TARGET


MOBILE SENDER
DIRECT ATTACK
WEB TARGET


WEB SENDER
DIRECT ATTACK
MOBILE TARGET


WEB SENDER
DIRECT ATTACK
WEB TARGET

REAL WORLD EXAMPLES OF MOBILE PHISHING ATTACKS

According to Verizon's 2020 Mobile Security Index report, attacks are becoming more sophisticated and targeted. While mobile devices have basic security protocols in place to protect email applications, phishing threats are happening in multiple vectors.

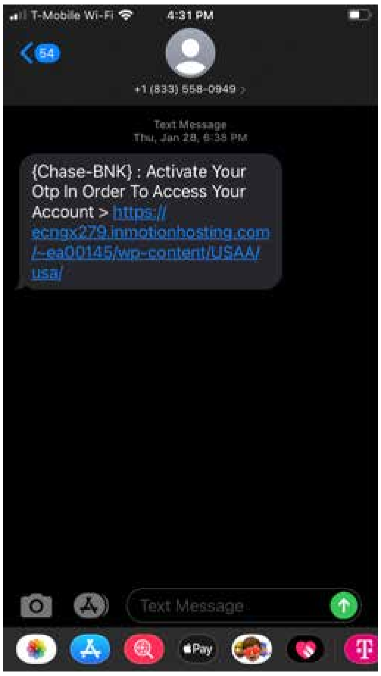
According to the same Verizon report, 85 percent of attacks seen on mobile devices took place outside of email.

Messaging – 17%
Social Media – 16%
Gaming – 11%
Productivity Apps – 10%
Others, including news and travel apps – 31%

verizon✓

THE SHADOW VOICE SOCIAL ENGINEERING ATTACK: NEW LEVEL OF SOPHISTICATION

During this attack, users got a text message saying they had to install software to communicate with the bank securely. That software was malware. Even if any user got suspicious and was smart enough to call their bank, attackers used the malware, cut off that call, put a screen overlay on the top of the phone screen, and called a different number for the bad actors to continue that attack.



{Chase-BNK} : Activate Your Otp In Order To Access Your Account > https://ecngx279.inmotionhosting.com/~ea00145/wp-content/USAA/usa/

COVID-19 INFORMATION TRACKER ATTACK: TAKING ADVANTAGE OF A GLOBAL PANDEMIC

Threat intelligence firm Domain Tools revealed in a report in 2020 that attackers were deploying Android ransomware called CovidLock that claims to be a COVID-19 information tracker but is actually designed to lock victims' screens until they pay a ransom. Researchers with Avast issued an alert about cybercriminals are “releasing malicious apps that are masking themselves as fake COVID-19 tracking apps or even fake 'cures' for the disease. Also, new apps have appeared that aim to spread misinformation about the pandemic."

BRANDED MOBILE PHISHING ATTACKS: MOBILE BANKING PAYDAY

A 2019 phishing campaign involving the use of SMS messages to lure potential victims into disclosing their bank-account access credentials impacted banks and mobile users in many countries, including the US. Among these banks were Chase, HSBC, TD, Scotiabank, and CIBC. While the attack is currently offline, according to Lookout, which tracked the attacks, at least 4,000 unique IP addresses belonging to mobile users were discovered. Lookout said it is not sure how the victims were impacted financially because of a lack of visibility into how the attackers might have actually used the compromised credentials. The attack was entirely mobile-focused, from delivering messages via SMS to rendering the phishing sites as mobile banking logins.

There is only a 30% penetration of threat defense on mobile devices, according to Gartner’s Market Guide for Mobile Threat Defense. Yet most mobile device users still think they have the protection they need to be safe.

Gartner

RISK MANAGEMENT: WHAT'S AT STAKE

Even CEOs of companies have been the victims of phishing attacks, and those CEOs have access to incredibly valuable information and systems.

The U.S. Federal Bureau of Investigation (FBI) tracks Business Email Compromise (BEC) which starts with a phishing email and targets high-level business leaders. Using social engineering or stolen credentials, cyber-criminals have used legitimate email accounts to trick people into making wire transfers, according to FBI reports.

These criminals also target company records, wage and tax statements, and medical records. They use the information to con other individuals, file false tax returns, and sell Personally Identifiable Information (PII) used to commit health insurance fraud.

More than 26,000 victims of phishing scams were reported in 2018, including payroll diversion. Cybercriminals used phishing emails to trick employees into giving them their login credentials. The crooks used these stolen credentials to access employee's payroll accounts and change direct deposit information. Paychecks were diverted to accounts by the criminals. Often, payroll was sent to an untraceable prepaid credit card.

In 2019, the FBI estimated billions of dollars stolen in the past five years; in 2018 alone, more than $1.2 billion in losses was reported.

Phishing scams increased more than 136 percent over the past two years, reported in all 50 states. The FBI has traced stolen funds to China, Hong Kong, Mexico, Turkey, and the United Kingdom.

Evaldas Rimasauskas pleaded guilty to wire fraud after initiating a phishing scheme targeting execs at Facebook and Google in a campaign that cost an estimated $100 million.

Boards of Directors are now getting actively involved, and prioritizing cyber security to protect organizations from not only financial losses, but the cost to repair the damage, contact individuals that have had records compromised, and pay fines or face class-action suits.

ADVANCED MOBILE WEB SECURITY SOLUTIONS

Isoolate is transforming the nature of cybersecurity by liberating users with its application driven approach. With its patent pending unique isolation technologies, Isoolate seamlessly protects users, from web and SaaS application content borne threats, who work from anywhere, on any device, and over any network.

Remote isolation eliminates browser based zero-day malware and phishing attacks, on all mobile devices and operating systems, as well as desktops.

BENEFITS INCLUDE:

UNLIMITED PRODUCTIVITY

Isoolate unlocks the productivity giving users the freedom to browse any content on the web without compromise

REDUCED COMPLEXITY

Isoolate’s Remote Browser Platform reduces the complexity for end-users and the IT teams protecting them with advanced automation and algorithms

PHISHING PROTECTION

Highest protection level with embedded control

WEB THREAT PROTECTION

Sends risky or unknown URL's to cloud isolation to address potential threats

URL FILTERING

Applies enterprise policies regardless of where the end-user is or which mobile device they are using

DOWNLOAD/UPLOAD PROTECTION

Control uploads and downloads wherever employees are working, including on their mobile devices

CONCLUSION

With advanced software solutions like those available from Isoolate, enterprises, businesses, government agencies and other organizations can give their employees protection against mobile phishing threats by allowing them to "roam free" without having to worry about what happens if they do accidentally engage with a phishing scam. Because the end-user can only view a rendering of the web page, with no links or underlying code activated, their devices and the data, applications and assets they have on their device, including access to centralized organizational assets – attackers are stopped in their tracks.

> "Phishing has evolved into a massive problem that expands far beyond the traditional email bait and hook. On a small screen and with a limited ability to vet links and attachments before clicking on them, consumers and business users are exposed to more phishing risks than ever before. In a mobile-first world, with remote work becoming the norm, proactive defense against these attacks is critical."
>
> Phil Hochmuth, Program Vice President of Enterprise Mobility at IDC Research
>
> IDC
> *Analyze the Future*

ABOUT ISOOLATE

Isoolate, founded in 2018 in New York, NY, is transforming the nature of cyber security by liberating users with an “application to content” approach. With its patent pending unique threat isolation technologies, Isoolate seamlessly protects users, from web and SaaS application content-borne threats, who work from anywhere, on any device, and over any network. For more information, visit **www.isoolate.com** or **https://www.linkedin.com/company/isoolate/**

Contact Us
selcan@isoolate.com