Briefing Note

DNS over HTTPS - Your Anti-Phishing Solution is About to Go Dark

Introduction

With over 46,000 new websites created every day, phishing continues to rise as one of the greatest threats currently facing mobile devices. Our phones are quickly becoming our most important means of communication and entertainment, but as technology has become more advanced, so too has the sophistication and frequency of phishing attacks. Taking advantage of the multiple platforms available, phishing campaigns can take many different forms on mobile, targeting users through email, SMS, social media and apps. With minimal effort and convincing fake login pages, hackers can easily trick users into revealing personal information including usernames, passwords and bank details.

In response to this rising threat, a number of cybersecurity vendors have developed anti-phishing solutions for mobile. These solutions detect and block phishing sites by examining (commonly referred to as 'sniffing') DNS traffic. This relies on the fact that today the vast majority of DNS traffic is transmitted 'in the clear' i.e. without encryption. However this is about to change with growing support from companies such as Google and Mozilla for DNS over HTTPS, a new method of domain name requesting that encrypts all data. So what does this mean for today's anti-phishing solutions?

What is DNS and DNS 'sniffing'?

DNS

DNS (Domain Name System) is the internet's system for converting alphabetic domain names into the numeric IP addresses that computers use to identify each other on a network. When a web address (URL) such as www.example.com is typed into a browser, DNS servers return the IP address in a numeric format like 204.0.8.51, and allow the user to retrieve the website associated with it. This makes it easier for users to browse the internet and find the information they are looking for, without the need to remember long series of numbers.

DNS Sniffing

Typically, DNS requests are sent in plain text. This enables the process of DNS 'sniffing' which allows bodies such as internet service providers (ISPs), security solution providers, and governments to capture, analyze and monitor requests sent and sites visited by users. DNS sniffing is used to analyze network usage, troubleshoot issues, and ensure compliance with content restrictions. However, this process has caused some concern over the safety and privacy of user data. Due to the nature of plain text data and how easily DNS requests can be sniffed, data gathered from tracking DNS traffic can be abused or become dangerous in the wrong hands. This has led to the introduction of DNS over HTTPS.

What is DNS over HTTPS?

DNS over HTTPS (DoH) and the closely related, DNS over TLS (DoT), work in much the same manner as regular DNS. However, rather than using plain text, the DNS query is sent to a DoH-compatible server via an encrypted HTTPS connection. This way, the DNS queries are hidden inside regular HTTPS traffic so that third-party observers are unable to sniff traffic or monitor what DNS queries users have run, consequently hiding whatever websites they are about to visit. DoH also works at app level as mobile apps can come with internally hardcoded lists of DoH compatible DNS resolvers where they can send queries. This allows app requests to bypass the default DNS settings that exist at OS level, and avoid local ISPs' traffic filters and content blocks. Due to this encryption and the reduction of restrictions, DoH has generally been hailed as essential for user privacy and security. Man-in-the-middle (MiTM) attacks often exploit the insecure nature of DNS via DNS Spoofing attacks, DNS Hijacking or DNS Poisoning which allow hackers to redirect webpage requests and return spoofed sites that appear to be legitimate. However, by putting DNS in a HTTPS encrypted channel, eavesdropping on DNS queries and MiTM attacks becomes much more difficult.

Objections to the changes

Despite the aforementioned benefits, not everyone is happy with the proposed changes. After it was announced that Google and Mozilla would be supporting DoH, there was an outcry from many cybersecurity and internet service providers. The trade association for ISPs in the UK even nominated Mozilla for the 'Internet Villain' of the year award. In the UK, ISPs are legally forced to block certain types of websites, for example those that mis-use copyrighted or trademarked content. What's more, some ISPs choose to block other 'inappropriate' or 'unsavory' content such as extremist views, adult images or child pornography. They argue that implementing DoH will significantly impact their ability to filter traffic on these 'bad sites'. Internet security providers have also protested these changes saying that encrypting traffic will prevent them from being able to sniff for potentially malicious and phishing websites. They argue that losing this power will lead to reduced data security for customers, as attackers love to hide in encrypted traffic, as it was a loss of visibility like this that played a part in the notorious Equifax data breach.

Despite these protests, it seems that the implementation of DoH will be going ahead with two of the world's biggest and most popular web browsers: Google Chrome and Mozilla Firefox.

As well as this, in the most recent Android release (Android 9), Google extended DoH support to the world's most popular mobile platform. Both companies maintain that although content filtering may become more complicated, and perhaps more expensive, it is worth supporting a tool that brings privacy improvements to millions at the expense of a few that may have to suffer.

Key Takeaways for users of anti-phishing protection solutions

Most anti-phishing solutions on the market today rely on DNS sniffing in order to monitor user traffic and block access to suspicious or malicious sites. With the introduction of DoH and encryption, this method will no longer be possible meaning that many anti-phishing solutions will be rendered useless. If you have a solution, ask your supplier how they intend to address this issue. If you are looking into an anti-phishing solution, be sure to ask prospective vendors about encrypted DNS traffic and how this will affect their mobile phishing protection.

Fortunately, Corrata has never relied solely on examining unencrypted DNS traffic to identify malicious activity. From its first release, Corrata Security and Control implemented comprehensive inspection of all IP traffic. Corrata's SafePathML technology is designed specifically to provide the highest level of visibility and protection on mobile. Doing this required the Corrata engineering team to solve a wide range of technically challenging issues and led Corrata to create the first ever enterprise grade firewall for mobile. With a robust solution now available which future proofs our customers against changes such as DNS over HTTPS, it is clear that the investment is now paying off providing comprehensive protection for our end users.

Want to find out more about these changes and ensuring your mobile devices are protected from phishing and other mobile threats?
Contact Corrata today