RESEARCH REPORT

Living with ECH

corrata

Introduction

Late last year, our security research team noticed an uptick in detections of the domain cloudflare-ech.com across our customer base.

The numbers were small - low thousands among hundreds of millions of domain scans - but nonetheless intriguing. Did this herald the primetime arrival of Encrypted Client Hello (ECH), a protocol which Information Security professionals feared would make widely used security tools blind to large swaths of internet traffic?

It was readily apparent that the spike in cloudflare-ech.com detections was directly related to internet infrastructure provider Cloudflare's decision to support ECH by default on its most popular plan. Our researchers wanted to investigate whether this change represented a tipping point in ECH adoption or just a small step change related to the policy of a single infrastructure provider.

Encrypted Client Hello (ECH) is an extension to the TLS 1.3 internet encryption standard. TLS, or Transport Layer Security, is the standard used to safeguard communications between an endpoint device and the web server it's connected to. It is the standard indicated by the familiar padlock symbol in browsers and the https designation in front of web addresses. TLS now protects the vast majority of internet traffic - a variety of sources put current adoption well above 90%. Of that traffic the vast majority uses TLS 1.3, the most recent version of the standard.[1]

ECH is designed to increase user privacy by encrypting the content exchanged between clients and servers when they are establishing the encrypted connection. Without ECH a client will reveal the domain of the website it is attempting to visit before the encrypted connection is established by disclosing the domain's Server Name Indicator (SNI). This means that any entity with visibility of a user's internet traffic (for example an Internet Service Provider (ISP), mobile operator, enterprise security teams, and/or bad actors), can see that user's destination even when the user and the server take precautions to avoid this.

Increased user privacy - what's not to like? Unfortunately in the view of many enterprise information security professionals,[2] increased privacy will come at the cost of compromising their ability to detect and respond to threats. Appliances such as Secure Web Gateways and Next Generation Firewalls rely on visibility of the SNI in order to identify the destination of traffic which would otherwise be hidden because of the use of encrypted dns and network edge services like Cloudflare. Widespread adoption of ECH would severely curtail the ability of enterprises to identify and block connections to malicious domains. A particular problem arises for regulated industries who need to selectively decrypt TLS traffic for compliance purposes: unable to do so selectively, they may have little choice but to decrypt all of it. Given the likely impact, it is important that we have a clear understanding of the current state and likely future trajectory of the rollout of ECH.

[1] See for example Google Transparency Report and Cloudflare Radar

[2] See here

Background

Transport Layer Security has revolutionized the confidentiality of internet communications. Before widespread use of encryption many legitimate and illegitimate actors had the potential to snoop on internet traffic, and even modify it.

However information 'leakage' remains: some is inherent to the how the internet works (e.g., source and destination addresses and other networking metadata will always remain 'in the clear') but other leakage is due to privacy gaps in the protocols. Two of these are of particular importance: client dns queries and TLS client hellos.

DNS queries are the way a device translates a request to visit a named website (e.g. google.com) into the IP addresses (e.g., 74.125.197.113) it needs to connect to the site. It sends the query to a DNS resolver - normally one which is provided by its ISP. In general these DNS requests are sent 'in the clear' meaning that the ISP and anyone else with access to the traffic can see the website the user is looking to access. ISPs, Governments and Enterprise IT teams can use this information to block access to sites deemed unacceptable or malicious. Encrypted DNS (i.e., DNS-over-TLS, DoT, or DNS-over-HTTP, DoH) is a way for users to hide this information. Typically they do this by replacing the default DNS on their device with an encrypted service such as 1.1.1.1 (Cloudflare) or 8.8.8.8 (Google). All major operating systems and browsers can be configured to use encrypted DNS. Corrata estimates that circa 20% of enterprise devices use encrypted DNS (EDNS).

EDNS is not turned on by default for a number of reasons. ISPs have a commercial interest in understanding how their subscribers use the internet. Access to DNS queries is very useful in this regard. Governments also have an interest in being able to passively monitor and potentially restrict access to illegal, malicious, or unacceptable content. Enterprise Information Security teams also have legitimate reasons for wanting to block access to content that could represent a threat, for example phishing or malware download sites. Device manufacturers want their devices to work seamlessly in all environments and are reluctant to turn on a feature which might lead to a poor user experience in some circumstances.

Unfortunately for those users who want to hide their internet activity from prying eyes, even with EDNS enabled, they cannot remain private. This is because of the information which is exchanged when their device establishes a TLS connection to the server it wants to access. The TLS "client hello" message sends the domain name of the server they are connecting to 'in the clear', making it visible to any entity monitoring network traffic. It is this gap which Encrypted Client Hello attempts to address.

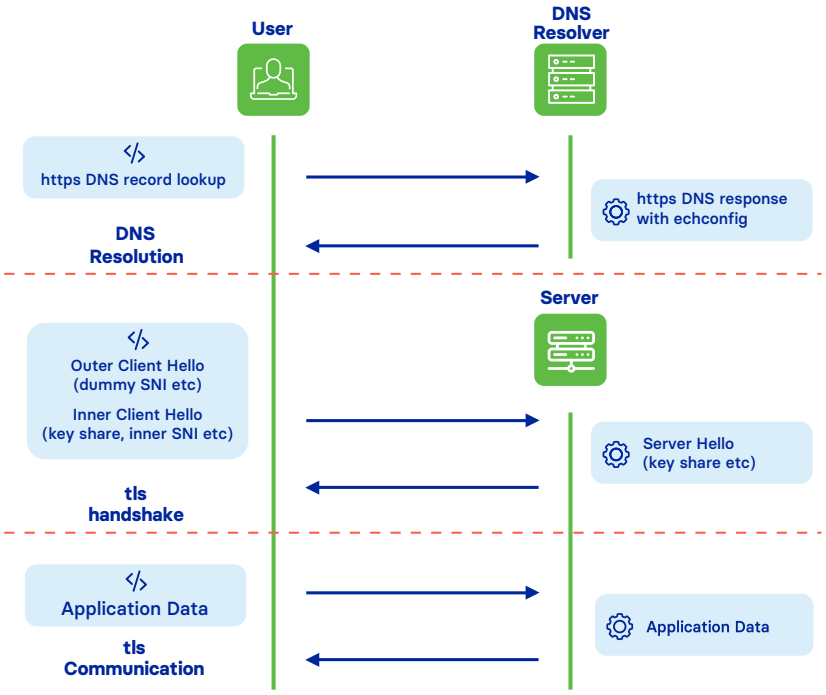
How Encrypted Client Hello works

Encrypted Client Hello (ECH) works by encrypting the Client Hello message, which is the first message sent by a client in a TLS handshake. Traditionally, this message—including the Server Name Indication (SNI)—is sent in plaintext, allowing network observers to see which specific domain a user is trying to access, even when the rest of the connection is encrypted.

ECH addresses this by encrypting the entire Client Hello using a public key obtained via DNS, specifically through the HTTPS resource record (type 65). The client sends an outer Client Hello with a benign or shared SNI and includes the encrypted inner Client Hello as an extension. Only the gateway to the intended server, which holds the corresponding private key, can decrypt this inner message and complete the handshake securely.

It should be noted that this necessarily depends on ECH enabled traffic being mixed with other ECH traffic going to different servers, but through the same gateway. Otherwise no privacy gains are achieved. This means that, in order to achieve its goal, ECH requires traffic to go through gateways controlled by large Content Delivery Networks (CDN), such as Cloudflare, who will still have access to the SNI. The privacy gains are therefore limited.

OVERVIEW OF ENCRYPTED CLIENT HELLO



In our research, all outer Client Hello messages observed used the same SNI: cloudflare-ech.com. This was true whether or not the website used Cloudflare infrastructure. This makes all websites using ECH indistinguishable from each other. This is possible because the content of this field plays no part in the TLS handshake.

ECH adoption in practice

For a website owner to offer ECH natively they will need to use a name server and a TLS stack that supports it. Today that support is limited, and for this reason the simplest way to enable ECH on your website is to work with a CDN that supports it.

In practical terms that means using Cloudflare. For an end-user to take advantage of ECH they will need to use a browser (e.g., Chrome, Firefox) that supports it. They will also need to configure their browser/device to use Encrypted DNS both to hide their DNS queries and to access an ECH compatible resolver such as 1.1.1.1 (Cloudflare) or 8.8.8.8 (Google)

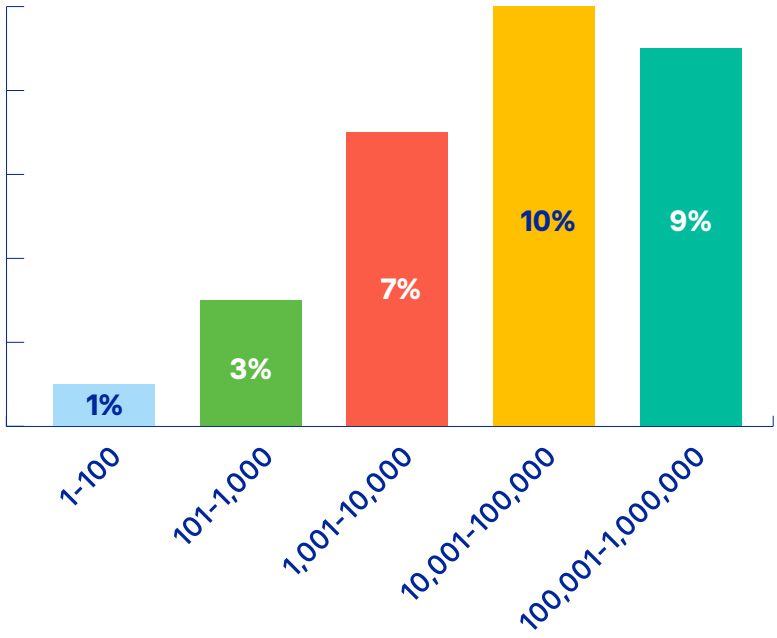
Our research aimed to establish how often these conditions apply to enterprise traffic. Our findings are based on analysing billions of connections made by devices running Corrata's threat detection and response solution. Corrata's software is used to protect iOS and Android devices and is representative of that important segment of enterprise internet traffic. Corrata has visibility of DNS query and TLS connection metadata for all of these connections and has tracked the number of successful ECH connections created between January and March 2025.

Of the top 1 million websites, slightly less than 10% support ECH. With a tiny number of exceptions, all of these sites use Cloudflare infrastructure, underlining the importance of Cloudflare for ECH adoption but also highlighting the lack of support from other infrastructure providers.

Looking at the end user side we see major gaps in potential ECH support. The first 'carve out' is for Apple devices: iOS does not support ECH. On Android devices, we see that 30% of users have both configured their browser/device to use encrypted DNS and are using a browser (Chrome in the vast majority of cases) that is ECH compatible.

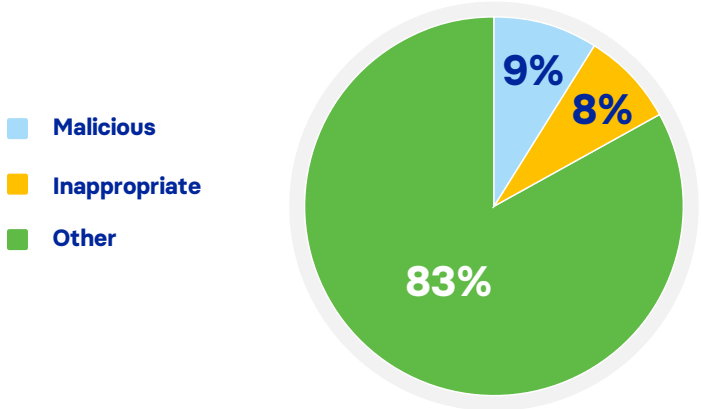
Taking the server and client support proportions together would suggest 2% of connections might be using ECH. In reality our data shows that only 0.06% of connections actually use it. This 'underperformance' is due to the fact that Cloudflare sites are not distributed evenly across the popularity tiers. Coverage falls to 3% when you look at the top 1,000 sites and 1% in the top 100 sites.

ECH SUPPORT BY SITE RANKING FOR THE TOP ONE MILLION SITES



The Cloudflare ECH site population exhibits other characteristics. Malicious and risky sites are heavily overrepresented - in total about 17% of ECH enabled sites are in these categories. Our analysis of phishing detections shows that over 90% use Cloudflare infrastructure. In addition to the anonymity provided by ECH, these sites take advantage of other Cloudflare features. For example the 'captcha' page can be used to direct desktop traffic to the legitimate site while mobile traffic is sent to the fake one. Alternatively, traffic not coming from the targeted country may be redirected to the legitimate site. These are deliberate tactics to avoid detection by security providers.

CATEGORY OF ECH SITES



Where to from here

The combination of the low levels of traffic which use ECH together with the high level of malicious and risky sites within the ECH enabled population will persuade many organizations to block access to sites using ECH absent any further knowledge of the content of the site.

Such an approach is defensible from a user experience perspective while ECH support remains at the low levels we have identified in our research. How quickly might that change?

Adoption can be driven from either the client or the server side. There are a number of factors which would drive adoption on the client side. The first would be for Safari to support the standard. Private Relay is Apple's subscription-based privacy-enhancing technology and it is unlikely to proactively support a potential alternative. A second would be for Chrome to enable encrypted DNS by default. This is more likely - Google would lose nothing with such an approach and it might disadvantage competitors who are seeking to monetise internet usage information. Our estimate is that were Chrome to make encrypted DNS a default it would likely double the proportion of TLS connections using ECH. But such a change would be a significant market intervention and would not be welcomed by mobile carriers who have influence over Google due to their role in handset sales.

The position in relation to Android is also not positive from an ECH adoption perspective. To understand why we must first look at how encrypted DNS is handled at the device wide level in Android. No major manufacturer has enabled DNS encryption by default. Users have the option to turn on "Private DNS"; once enabled, the device will encrypt all DNS queries using the DNS-over-TLS (DoT) standard. However device-wide DoT is not properly compatible with ECH for a variety of reasons. Furthermore the TLS stack within Android would also need to be enhanced to support ECH to allow the 90% of connections which are not browser related to make use of the privacy enhancing standard.

For server side adoption to increase you would need to see wholesale migration to Cloudflare (unlikely) or default support from other Content Delivery Networks. 23.6% of the top 15 million websites use a CDN. This understates their importance as CDN penetration is particularly high among the most popular sites. The market is dominated by Cloudflare, Fastly, Amazon and Akamai.[3] CDNs other than Cloudflare have so far announced only tentative steps towards ECH support with no suggestion of default enablement. That said, ECH adoption is a positive for the CDNs. The complexity of implementation means more websites will opt to use CDN services. At a more strategic level, the CDNs would become the only infrastructure players with widespread visibility of end-user application usage.

[3] Merrill and Narechania, Inside the Internet, Duke Law Journal Online

Conclusion

The spike in detections of the cloudflare-ech.com domain observed in the latter part of 2024 was the catalyst for this research. We wanted to understand what the implications of this new phenomenon might be for enterprise information security.

A rapid increase in the use of Encrypted Client Hello would mean that it would no longer be possible to directly detect the destination of much internet traffic. Security tools designed to keep enterprises safe would lose some of the visibility they rely on.

Our findings indicate that this 'visibility apocalypse' is not in fact imminent. The fact that large elements of the ecosystem are not moving to quickly support ECH means that the low levels of penetration we see today are not likely to change rapidly. There are major gaps on both the client and infrastructure side. On the client side you need support for both DoH and ECH. Device wide support for this combination is non-existent for Android and iOS and this is unlikely to change in the short to medium term. Lack of support from Safari is a big gap on the browser side. Chrome offers support for DoH and ECH but not by default.

On the infrastructure side Cloudflare is the only provider supporting ECH today. Cloudflare's promotion of the standard is part of its privacy-first positioning and support is baked into its tech stack. Other providers are not in the same market or technical position. It would be complacent to expect this position to continue longer term as ECH adoption offers significant market opportunities for the CDN industry. . For now information security professionals can breathe a sigh of relief. But continuing to track this space is no longer optional.

Authors

This research was conducted by Matthieu Bentot, CTO and Creagh Duggan, Security Analyst.

corrata

Corrata provides endpoint threat detection and response for mobile. Our pioneering architecture delivers real-time visibility into threats targeting both iOS and Android devices, without compromising performance or privacy. Corrata has customers across multiple verticals including healthcare, logistics, manufacturing and the public sector and is verified for use with FirstNet, the US Government network for first responders.

For more information, please contact the Corrata team at **info@corrata.com**

corrata

corrata.com