TEAM CYMRU

***Team Cymru Myth vs Fact***

MYTHS *Myth: Team Cymru is a 'data broker'*

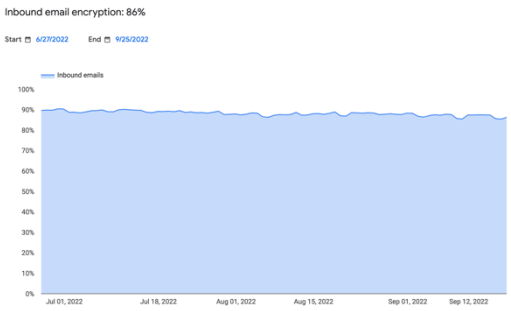
FACTS ***Fact: We are not a data broker.***

*Our focus is on compromised and malevolent Internet devices, not on persons. We hold no subscriber data that would allow any users of our product to connect a person to a piece of Internet infrastructure. The data that underpins our product is lawfully handled and compliant with all applicable data privacy regulations, including GDPR, CCPA and other relevant state and national privacy legislation. Our platform doesn't show the type, usage or users of Internet services.*

MYTHS *Myth: The Augury platform makes a wide array of different types of internet data available to its users, including packet capture data (PCAP) related to email, remote desktop, and file sharing protocols.*

FACTS ***Fact: Our platform does not collect email, remote desktop or file sharing (FTP, torrents, et al.) on the Internet.***

*Numerous studies have shown that the collection of email is not possible because the vast majority of email is encrypted end-to-end. In a September 2022 Google report it was shown that 75% of outbound email and 86% of inbound email is encrypted in transit. Email to and from many providers, such as Google, Microsoft, Cloudflare, Amazon, Comcast, Apple iCloud, Facebook, LinkedIn, Twitter, Instagram, and Protonmail, is encrypted in transit by default via TLS, without any user configuration required. According to Microsoft, Remote Desktop Protocol (RDP) has been encrypted by default since 2009.*



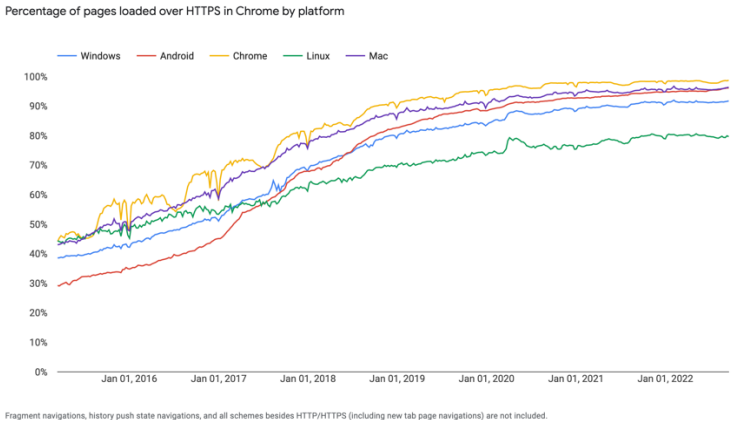

*We extract malicious email addresses (not content), remote desktop attempts, and FTP attempts through our malware sandboxing, and we report spam and phishing from our spam traps and honeypots. All of our PCAPs are generated in our internal infrastructure.*

MYTHS *Myth: "Augury's data can also include web browser activity, like URLs visited and cookie usage."*

FACTS ***Fact: Our platform isn't capable of global web traffic collection and presentation. Our platform only provides URLs and cookies mapped to malicious servers.***

*Studies have proven such collection activity simply isn't possible. The web is an encrypted sphere, keeping web traffic safe from prying eyes. Google's transparency study shows that over 90% of page loads via their Chrome browser are encrypted over HTTPS. In Google's review of the top 100 web sites, which account for 25% of all global*

*web traffic, 100 out of 100 of those sites provide encryption, and 97 of them default to encryption. Scott Helme has performed checks of the Alexa top one million web sites, and showed that 72% of the top one million web sites defaulted to encryption. The CA Security Council predicted that over 90% of web traffic would be encrypted by May 2019, presciently matching Google's current findings. The Firefox Telemetry project concluded that 87% of all page loads by Firefox browsers were encrypted.*




*Yet there are compromised websites, with the Webtribunal study of April 2022 noting that 1 in 10 URLs are malicious. IBM noted in 2020 that 30,000 web sites are hacked each day. Through our malware analysis engines, scanners, honeypots, spam traps, phishing detection, IDS platform, and feeds of IOCs (indicators of compromise) we identify compromised websites. These sites spread malware, command armies of bots and launch attacks, in addition to stealing credentials. Network defenders want to spot, block, or clean these devices and related infected devices as quickly as possible. Our platform makes it possible to see these hacked sites. This data is tied solely to malicious activity and malicious infrastructure, and the network defenders who use our tools rely on it to better defend their infrastructure.*

MYTHS *Myth: Team Cymru obtains PCAP data from the Internet Service Providers (ISPs) it has relationships with.*

FACTS ***Fact**: **We do not obtain PCAP data from any 3rd party.***

*We invest significant resources towards running our own global platform of honeypots, IDS sensors, scanners, and numerous malware processing engines. Our infrastructure is the source of our data. This data forms the basis of our products and services, including services such as our free to use CSIRT (Computer Security Incident Response Team) Assistance Program and the Malware Hash Registry (MHR). CSIRT teams in over 140 countries download our threat intelligence daily. Millions of queries hit our publicly available insight portals, and our customers use our feeds and platforms to defend their networks. Our stellar reputation results from two decades of partnership with the communities and network defenders.*

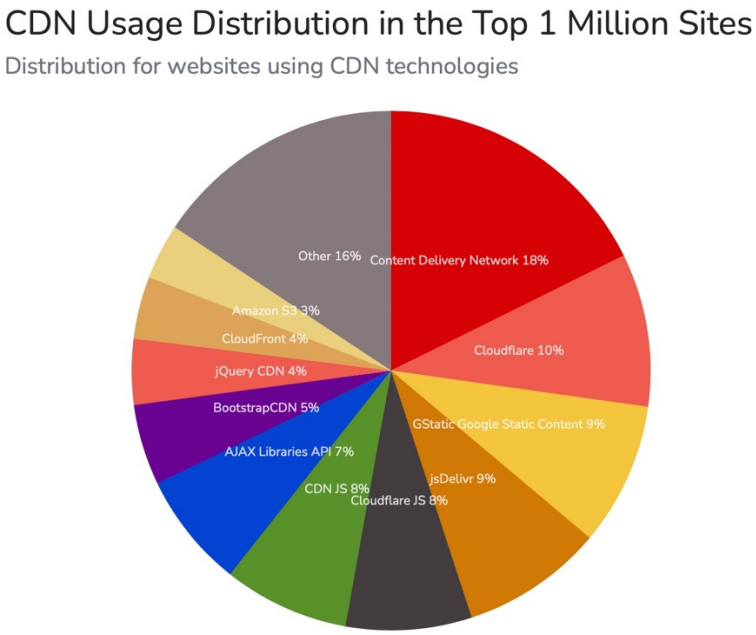
MYTHS *Myth: "Augury also contains so-called netflow data … Netflow records can reveal which servers users connect to, often thereby revealing*

*specific websites they visit. The logs may also reveal the volume of data sent or received, and how long a user accessed a site."*

FACTS

***Fact**: **Augury does not provide anyone access to raw or bulk netflow data**. **Netflow records contain no content or user information. It is statistically inaccurate to assert that netflow can be used to identify an individual or provide a pattern of life that can be mapped to a person and preferences.***

*Limited, specific queries producing anonymized and aggregated results can be derived from sampled netflow. Netflow does not identify users. Netflow data includes only headers such as protocol and device IP addresses. It is sampled and thus sees only approximately 1 in every 10,000 netflow. These sessions include scanning, hacking, ddos, and other forms of malicious activity. Further, legitimate sessions are driven through content delivery networks (CDN) behind which sit millions of websites. Of the top 1M websites, 43.96% sit behind CDNs, 59.04% of the top 100K websites and 61.95% of the Top 10K websites. It is impossible to use netflow to differentiate between these websites. Additionally, shared infrastructure among cloud providers further precludes identifying specific cloud hosted infrastructures. It is thus statistically inaccurate to assert that netflow can be used to identify an individual or provide a pattern of life that can be mapped to a person and preferences. There are no logs or any content included in netflow.*




*Malicious controllers, large scale scans, and DDoS have a persistence and periodicity that reveals a statistical pattern, permitting the mapping of malicious infrastructures and identifying hacked devices of importance to network defenders. Augury enables the mapping of malicious devices, not people. Please see our Nimbus Threat Monitor and other Community services for additional details. https://www.team-cymru.com/community-services*


*Myth: Augury provides different levels of access for private (commercial) and government clients.*


***Fact**: **False. There is one identical platform with usage-based tiers.***

*Endnote*

[1] https://en.wikipedia.org/wiki/Information_broker
[2] https://transparencyreport.google.com/safer-email/overview?hl=en
[3] https://scotthelme.co.uk/top-1-million-analysis-november-2021
[4] https://techcommunity.microsoft.com/t5/security-compliance-and-identity/top-10-rdp-protocol-misconceptions-8211-part-2/ba-p/246716
[5] https://transparencyreport.google.com/https/overview?hl=en
[6] https://scotthelme.co.uk/top-1-million-analysis-november-2021
[7] https://vmblog.com/archive/2019/01/10/ca-security-council-2019-predictions-the-good-the-bad-and-the-ugly.aspx
[8] https://telemetry.mozilla.org
[8] https://webtribunal.net/blog/ssl-stats/
[9] https://community.ibm.com/community/user/security/blogs/lissa-coffeey1/2020/11/30/global-website-hacking-statistics-in-2020
[10] https://trends.builtwith.com/cdn
[11] https://www.team-cymru.com/community-services