Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data

Joseph Cox ⋮ 15-19 minutes ⋮ 9/21/2022

Multiple branches of the U.S. military have bought access to a powerful internet monitoring tool that claims to cover over 90 percent of the world's internet traffic, and which in some cases provides access to people's email data, browsing history, and other information such as their sensitive internet cookies, according to contracting data and other documents reviewed by Motherboard.

Additionally, Sen. Ron Wyden says that a whistleblower has contacted his office concerning the alleged warrantless use and purchase of this data by NCIS, a civilian law enforcement agency that's part of the Navy, after filing a complaint through the official reporting process with the Department of Defense, according to a copy of the letter shared by Wyden's office with Motherboard.

Videos by VICE

The material reveals the sale and use of a previously little-known monitoring capability that is powered by data purchases from the private sector. The tool, called Augury, is developed by cybersecurity firm Team Cymru and bundles a massive amount of data and makes it available to government and corporate customers as a paid service. In the private industry, cybersecurity analysts use it for following hackers' activity or attributing cyberattacks. In the government world, analysts can do the same, but agencies that deal with criminal investigations have also purchased the capability. The military agencies did not describe their use cases for the tool. However, the sale of the tool still highlights how Team Cymru obtains this controversial data and then sells it as a business, something that has alarmed multiple sources in the cybersecurity industry.

"The network data includes data from over 550 collection points worldwide, to include collection points in Europe, the Middle East, North/South America, Africa and Asia, and is updated with at least 100 billion new records each day," a description of the Augury platform in a U.S. government procurement record reviewed by Motherboard reads. It adds that Augury provides access to "petabytes" of current and historical data.

Motherboard has found that the U.S. Navy, Army, Cyber Command, and the Defense Counterintelligence and Security Agency have collectively paid at least $3.5 million to access Augury. This allows the military to track internet usage using an incredible amount of sensitive information. Motherboard has extensively covered how U.S. agencies gain access to data that in some cases would require a warrant or other legal mechanism by simply purchasing data that is available commercially from private companies. Most often, the sales center around location data harvested from smartphones. The Augury purchases show that this approach of buying access to data also extends to information more directly related to internet usage.

Team Cymru says on its website that its solution provides "access to a super majority of all activity on the internet."

Do you work at a company that handles netflow data? Do you work at an ISP distributing that data? Or do you know anything else about the trade or use of netflow data? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, or email joseph.cox@vice.com.

"Augury is the visibility into 93% of internet traffic," another website describing the tool reads. Some clients have access to the platform under the different brand name Pure Signal RECON, according to Team Cymru's website.

The Augury platform makes a wide array of different types of internet data available to its users, according to online procurement records. These types of data include packet capture data (PCAP) related to email, remote desktop, and file sharing protocols. PCAP generally refers to a full capture of data and encompasses very detailed information about network activity. PCAP data includes the request sent from one server to another, and the response from that server too.

PCAP data is “everything,” Zach Edwards, a cybersecurity researcher who has closely followed the data trade, told Motherboard in an online chat. “It’s everything. There’s nothing else to capture except the smell of electricity.” (Team Cymru told Motherboard it does limit what data is returned to users but did not specify what data actually is provided to a user of the platform.)

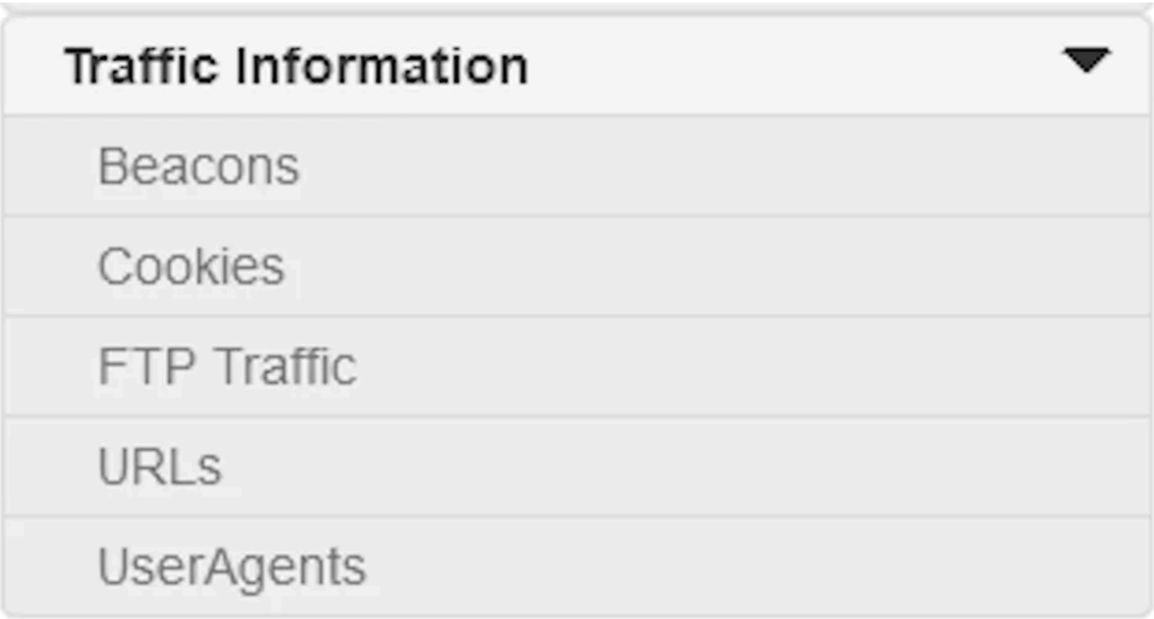
A source in the cybersecurity industry said “that’s insane” when shown that sensitive information like PCAP data was available in Augury. Some private industry users appear to have less access to certain data types in Augury than those listed in the government procurement records. Motherboard granted multiple sources in this piece anonymity because they weren’t authorized by their employers to speak on this issue.

Augury’s data can also include web browser activity, like URLs visited and cookie usage, according to the procurement records. Cookies are sensitive files that websites plant onto computers when people visit them. Given their uniqueness, cookies can be effective for tracking. Facebook and Google, for example, use cookies to follow a particular user from website to website and track their activity. The NSA has then piggybacked off of these cookies to identify targets for hacking. Screenshots of an apparent Augury panel obtained by Motherboard show results containing cookies, URLs visited, and email data. Motherboard showed a section of one of the screenshots to multiple sources familiar with the tool who said it does appear to be the Augury panel.

Augury also contains so-called netflow data, which creates a picture of traffic flow and volume across a network. That can include which server communicated with another, which is information that may ordinarily only be available to the server owner themselves or to the internet service provider carrying the traffic. That netflow data can be used for following traffic through virtual private networks, and show the server they are ultimately connecting from. Multiple sources in the cybersecurity industry told Motherboard that netflow data can be useful for identifying infrastructure that hackers are using.

Team Cymru obtains this netflow data from ISPs; in return, Team Cymru provides the ISPs with threat intelligence. That transfer of data is likely happening without the informed consent of the ISPs’ users. A source familiar with the netflow data previously told Motherboard that “the users almost certainly don’t [know]” their data is being provided to Team Cymru, who then sells access to it.

It is not clear where exactly Team Cymru obtains the PCAP and other more sensitive information, whether that’s from ISPs or another method.



A screenshot of Augury obtained by Motherboard. Image: Motherboard.

Motherboard asked Team Cymru multiple times if Augury contains cookies, URLs visited, and PCAP data, as the procurement records show. Team Cymru did not answer the question directly, and instead wrote in an email that “The Augury platform is not designed to target specific users or user activity. The platform specifically does not possess subscriber information necessary to tie records back to any users.”

“Our platform does not provide user or subscriber information, and it doesn’t provide results that show any pattern of life, preventing its ability to be used to target individuals. Our platform only captures a limited sampling of the available data, and is further restricted by only allowing queries against restricted sampled and limited data, which all originates from malware, malicious activity, honeypots, scans, and third parties who provide feeds of the same. Results are then further limited in the scope and volume of what’s returned,” Team Cymru said in another email.

Some have used Team Cymru’s data as part of investigations that aimed to identify specific computers and then contact the person using it, though. In July 2021 researchers at Citizen Lab published a report about Israeli spyware vendor Candiru. As part of that, the researchers wrote that they used Team Cymru’s data to identify a computer they believed had been infected with Candiru’s malware, and in turn, contacted the owner of that computer. Citizen Lab did not respond to a request for comment.

The procurement record that says Augury has access to PCAP data, URLs visited, and cookies relates to the maintenance of a Department of the Navy purchase of the tool. Other procurement data viewed by Motherboard shows the Department of the Navy paid for a “Platinum” Augury license. Beyond that, it is not clear which of Team Cymru’s U.S. government clients have access to the more sensitive data such as cookies. Records for the Army, Cyber Command, and the Defense Counterintelligence and Security Agency do not explicitly include the “platinum” marker, but in some cases the amount paid by the agencies is the same amount the Navy paid for a platinum license.

These sales to the U.S. government were made through a company called Argonne Ridge Group, which Motherboard found shares an address with Team Cymru. Team Cymru told Motherboard in an email that Argonne Ridge Group is an affiliate of Team Cymru which has historically handled contracts with public agencies.

Although they don’t explicitly mention Augury, Motherboard found multiple contracts between Argonne Ridge Group and the FBI and Secret Service. One of the FBI contracts says “it will secure funding approval to buy net flow from one commercial vendor and integrating it into existing sources of net flow available to cyber intelligence analysts to analyze as a proof of concept.” The Secret Service did not respond to multiple requests for comment. The FBI did not provide a response in time for publication.

The Army was unable to provide a statement on the Augury platform purchases in time for publication. After initially acknowledging Motherboard’s request for comment, the Defense Counterintelligence and Security Agency later deferred to the Department of Defense.

Charles E. Spirtos from the Navy Office of Information told Motherboard in an email that NCIS specifically “conducts investigations and operations in accordance with all applicable laws and regulations. The use of net flow data by NCIS does not require a warrant.” Spirtos added that NCIS has not used netflow during any criminal investigation, but that “NCIS uses net flow data for various counterintelligence purposes.”

Regarding the whistleblower that Senator Wyden says approached his office, their complaint relates specifically to use by NCIS, which Motherboard found does have a contract with Argonne Ridge Group.

“NCIS will defeat threats from across the foreign intelligence, terrorist and criminal spectrum by conducting operations and investigations ashore, afloat, and in cyberspace, in order to protect and preserve the superiority of the Navy and Marine Corps warfighters,” NCIS’ website reads.

In his letter addressed to the oversight departments of the DHS, DOJ, and DOD, Senator Wyden writes that “my office was recently contacted by a whistleblower who described a series of formal complaints they filed up and down their chain of command, as well as to the DOD Inspector General and the Defense Intelligence Agency, regarding the warrantless purchase and use of netflow data by the Naval Criminal Investigative Service (NCIS).”

The whistleblower alleges that NCIS is purchasing data from Team Cymru that includes both “netflow records and some communications content,” the letter continues. “The whistleblower has informed my office that their complaint was forwarded by the DOD Inspector General to the Navy Inspector General.” Pointing to the various U.S. government contracts for access to Augury, which his office also reviewed, in his letter Senator Wyden asks the oversight branches of the DHS, DOJ, and DOD to “investigate the warrantless purchase and use of Americans’ internet browsing records by the agencies under your jurisdictions. Your independent oversight must ensure that the government’s surveillance activities are consistent with the Supreme Court’s Carpenter decision and safeguard Americans’ Fourth Amendment rights.”

The Department of Defense Office of the Inspector General, which the whistleblower alleges referred their complaint to the Navy, told Motherboard it had received Wyden’s letter and was reviewing it. The Office of the Naval Inspector General declined to comment and directed Motherboard back to its Department of Defense counterpart.

Beyond his day job as CEO of Team Cymru, Rabbi Rob Thomas also sits on the board of the Tor Project, a privacy focused non-profit that maintains the Tor software. That software is what underpins the Tor anonymity network, a collection of thousands of volunteer-run servers that allow anyone to anonymously browse the internet.

“Just like Tor users, the developers, researchers, and founders who’ve made Tor possible are a diverse group of people. But all of the people who have been involved in Tor are united by a common belief: internet users should have private access to an uncensored web,” the Tor Project’s website reads.

When asked by Motherboard in April about Thomas’ position on the Tor Project board while also being the CEO of a company that sells a capability for attributing activity on the internet, Isabela Bagueros, executive director for the Tor Project, said in an email that “Rabbi Rob’s potential conflicts of interest have been vetted according to the standard conflicts disclosure process required of all board members. Based on the board’s understanding of Rabbi Rob’s work with Team Cymru, the board has not identified any conflicts of interest.”

Motherboard has previously revealed other data purchases by the U.S. military. In 2020, Motherboard found that a Muslim prayer app downloaded more than 98 million times sold its location data to a broker called X-Mode. X-Mode, in turn, included U.S. military contractors among its clients. As part of that investigation, Motherboard also found that U.S. Special Operations Command had purchased Locate X, a surveillance tool based on location data harvested from ordinary apps. Last March, Motherboard reported that a military unit that conducts drone strikes bought Locate X too.

After Motherboard published some of those findings, Sen. Wyden asked the Department of Defense for more information about its data purchases. Some of the agency’s subsequent responses were given in a form that meant Wyden’s office could not legally publish specifics on the surveillance; one answer in particular was classified. Instead, Wyden wrote in a second letter in May 2021 to the agency: “I write to urge you to release to the public information about the Department of Defense’s (DoD) warrantless surveillance of Americans,” suggesting that the Pentagon is engaged in such surveillance. At the time, Wyden’s office declined to provide Motherboard with specifics about the classified answer. But a Wyden aide said that the question related to the Department of Defense buying internet metadata.

In August, the House of Representatives approved changes to next year’s military budget that would require the Department of Defense to start to disclose any purchases of web browsing or smartphone data that would ordinarily require a warrant, *Gizmodo* reported at the time. It has yet to be approved by the Senate.

Other cybersecurity companies also package controversial datasets. In 2020 Motherboard reported that HYAS, a threat intelligence firm, sourced location data in order to track people to their “doorstep.”

Update: This piece has been updated with a statement from the Navy.

This article is part of State of Surveillance, made possible with the support of a grant from Columbia University’s Ira A. Lipman Center for Journalism and Civil and Human Rights in conjunction with Arnold Ventures. The series will explore the development, deployment, and effects of surveillance and its intersection with race and civil rights.