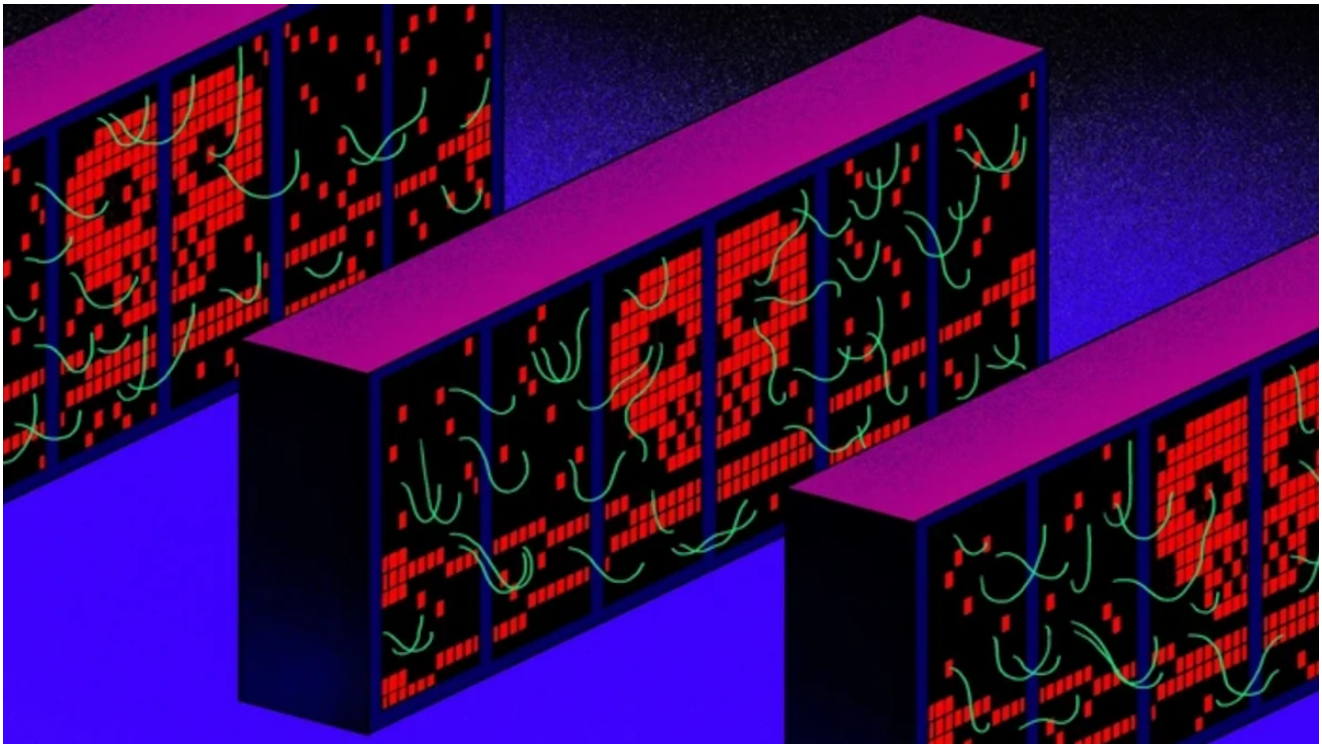
How Data Brokers Sell Access to the Backbone of the Internet

vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru



Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

See More →

There's something of an open secret in the cybersecurity world: internet service providers quietly give away detailed information about which computer is communicating with another to private businesses, which then sells access to that data to a range of third parties, according to multiple sources in the threat intelligence industry.

The information, known as netflow data, is a useful tool for digital investigators. They can use it to identify servers being used by hackers, or to follow data as it is stolen. But the sale of this information still makes some people nervous because they are concerned about whose hands it may fall into.

"I'm concerned that netflow data being offered for commercial purposes is a path to a dark fucking place," one source familiar with the data told Motherboard. Motherboard granted multiple sources anonymity to speak more candidly about industry issues.

At a high level, netflow data creates a picture of traffic flow and volume across a network. It can show which server communicated with another, information that may ordinarily only be available to the server owner or the ISP carrying the traffic. Crucially, this data can be used for, among other things, tracking traffic through virtual private networks, which are used to mask where someone is connecting to a server from, and by extension, their approximate physical location.

Team Cymru, one threat intelligence firm, works with ISPs to access that netflow data, three sources said. Keith Chu, communications director for the office of Senator Ron Wyden which has been conducting its own investigations into the sale of sensitive data, added that Team Cymru told the office "it obtains netflow data from third parties in exchange for threat intelligence."

> ***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 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.***

Companies that may source Team Cymru's data include cybersecurity firms hired to respond to data breaches or proactively hunt out hackers. On its website, Team Cymru says it works with both public and private sector teams to "to help identify, track and stop bad actors both in cyber space and on the ground."

"I'm less worried about a bad guy hacker and more worried about a bad guy government or company or politician," one source familiar with the data said. A source in the threat intelligence industry added that they "always thought it was kinda bonkers," referring to Team Cymru's sale of netflow data.

The continued sale of sensitive data could present its own privacy and security concerns, and the news highlights that ISPs are providing this data at scale to third parties likely without the informed consent of their own users. Other companies, such as cybersecurity firm Palo Alto Networks, also have access to netflow data.

"The users almost certainly don't [know]" their data is being provided to Team Cymru, who then sells access to it, the source familiar with the data said.

Tech

Private Intel Firm Buys Location Data to Track People to their 'Doorstep'

Joseph Cox

09.02.20

Team Cymru's customers can probe a dataset, and "effectively run queries against virtually any IP to pull the netflows to and from that IP over a given point in time," one of the sources said. Chu added Team Cymru said it "restricts the amount of data that is returned, so that only a small portion of the netflow data in its database can be accessed by any one client."

In product descriptions, Team Cymru offers users the ability to follow traffic through VPNs, which attackers may use to cover their tracks or ordinary people to browse the internet more privately.

"Trace malicious activity through a dozen or more proxies and VPNs to identify the origin of a cyber threat," one brochure for a Team Cymru product called Pure Signal Recon reads. In essence, access to netflow data lets a security team observe what is happening on the wider internet, and may indicate what is happening to other organizations, beyond the borders of their own network or company. One of the sources said they previously saw traffic from an organization they knew inside Team Cymru's dataset and was spooked by it at the time.

"Visibility and insight are global," the description adds. An image included in the brochure shows Team Cymru's product letting users trace the activity of servers linked to an Iranian hacking group further than other datasets, such as DNS lookups.

A section of Team Cymru's marketing material for its Pure Signal Recon product. Image: Team Cymru.

In a recent research report on an Israeli spyware vendor called Candiru, Citizen Lab thanked Team Cymru.

"Thanks to Team Cymru for providing access to their Pure Signal Recon product. Their tool’s ability to show Internet traffic telemetry from the past three months provided the breakthrough we needed to identify the initial victim from Candiru’s infrastructure," the report reads. Citizen Lab did not respond to multiple requests for comment.

Team Cymru did not respond to multiple requests for comment on which ISPs provide it with the data, what privacy protections are in place around the collection and distribution of such data, and whether the individual ISP users have provided consent for their data to be shared.

> "Fundamentally, people have a right to some degree of anonymity, and as a carrier it's not our job to eavesdrop in any form."

For its Cortex Xpanse product, Palo Alto Networks also gains access to netflow data, according to product documentation available online.

"Cortex® Xpanse™ obtains flow data via multiple relationships with Tier 1 ISPs. Through these relationships, Cortex Xpanse has access to a sample of approximately 80% of global flows," one page reads.

Jim Finkle, director of threat communications at Palo Alto Networks, said in an emailed statement that "Palo Alto Networks provides enterprise customers with netflow data to and from their own networks to identify violations of security policies, gaps in security monitoring and other high-risk activity on the customer's network." Palo Alto Networks declined to name which ISPs it sources data from, or whether it purchases the data outright from the ISPs.

Dave Schaeffer, CEO of ISP Cogent Communications, which he said handles around 22 percent of the world's internet traffic, told Motherboard that as an ISP his company doesn't provide their netflow data to anybody.

"Fundamentally, people have a right to some degree of anonymity, and as a carrier it's not our job to eavesdrop in any form," he said in a phone call. Schaeffer says Cogent generates 96 percent of its traffic from selling to large wholesale customers, such as Vodafone, Cox, Spectrum, and BT. Schaeffer says Cogent provides services to Team Cymru but does not share netflow data with the company.

"I don't know if there's a lot of really useful things people could do with [netflow] data," he added. "There's probably some bad things I could think of if that data was available."

Although multiple sources were concerned about the sale of netflow data, several of them stressed that Team Cymru is a responsible organization.

"It's pretty shadowy but honestly they're a 'good actor,'" one in the threat intelligence industry said. "Very strict protections on who can see it, but still, yeah, it's shady."

The source familiar with the data said they were concerned about the sale of netflow data, but that Team Cymru "also enable security organizations to do some really awesome work. So I'm conflicted about it."

> "I'm concerned that netflow data being offered for commercial purposes is a path to a dark fucking place."

In May, Motherboard reported that Senator Wyden's office asked the Department of Defense (DoD), which includes various military and intelligence agencies such as the National Security Agency (NSA) and the Defense Intelligence Agency (DIA), for detailed information on its data purchasing practices. The response showed that the Pentagon is carrying out warrantless surveillance of Americans, according to a subsequent letter written by Wyden and obtained by Motherboard.

Some of the answers the DoD provided were provided in a form meaning that Wyden's office could not legally publish specifics on the surveillance. Wyden's office then asked the DoD to release the information to the public. At the time, Wyden's office declined to provide Motherboard with specifics on one of the answers which was classified, but a Wyden aide said that the question related to the DoD buying internet metadata.

"Are any DoD components buying and using without a court order internet metadata, including 'netflow' and Domain Name System (DNS) records," the question read.

Other cybersecurity firms sell access to controversial datasets. In September, Motherboard reported how one firm called HYAS was sourcing smartphone location data to trace people to their "doorstep." As Motherboard has repeatedly shown, the ordinary apps installed on peoples' phones that gather this information often don't have informed consent to then sell or otherwise provide it to third parties.

Subscribe to our cybersecurity podcast CYBER, here.