BCAP NewsClips

May 29, 2015

The Internet's march toward media domination continues, and Netflix seems to be leading the way. The streaming-TV service now accounts for 36.5 percent of the total bandwidth consumed by North American users during peak traffic periods, up nearly two percent since November, according to the latest report by Canada-based network company Sandvine.

The report reflects a trend that has become clear in the last few years: Demand for Netflix, and online video in general, is growing at an incredible pace. How that will shape the content service industry remains a big unknown. Does the growth of Netflix and its ilk herald the death of cable TV, as consumers cut the cord in favor of streaming services? Or does it strengthen broadband providers – many of them cable companies – as online video services increasingly rely on fast, high-quality Internet? "Netflix no longer takes up just a third of Internet traffic anymore. Now it's edging closer to two-fifths," tech reporter Brian Fung **wrote in a blog** for The Washington Post.

Together, Netflix and YouTube already account for more than half all bandwidth consumed in North America, based on the Sandvine study. By 2019, video could represent up to 80 percent of the world's Internet traffic consumption, according to tech giant Cisco's annual report on the future of the web. "It would take an individual over 5 million years to watch the amount of video that will cross global IP networks each month in 2019," the report predicted. Or, as Mr. Fung succinctly put it, "Video is eating the Web." Less certain is who comes out on top as a result.

Yes, online video and streaming services are gaining serious ground. Netflix saw more

than 4 million new subscribers in the last quarter of 2014, bringing its total subscriber base to more than 57 million worldwide. About 40 percent of US homes now have access to subscription video on-demand (SVOD), according to Nielsen's Total Audience Report, released in March. Meanwhile, pay-TV providers lost about 125,000 net subscribers in 2014, up from 95,000 in 2013, according to New Hampshire-based media firm Leichtman Research Group. Live television watching was also on the decline, especially among younger audiences. In 2014, US adults spent, on average, just under 5 hours a day watching live TV, down 13 minutes from the year before, the Nielsen report found.

Still, that may not mean it's the end of the line for cable companies. Though more households now have SVOD access, more than 90 percent of those that have SVOD, broadband, and cable are more likely to hang on to cable than the first two, according to Nielsen. More significant, perhaps, is the growing pressure on online video services to stream more quickly and reliably. More users streaming more content puts a greater burden on Internet infrastructure, and can slow down services.

Last year, Netflix cut controversial deals, first with Comcast, and then with the next three largest American broadband Internet service providers, in which Netflix would pay for faster, more reliable streaming to their subscribers. "The [Netflix-Comcast] accord is the latest sign that broadband providers are gaining leverage with content companies," The Wall Street Journal noted. It remains unclear who will ultimately benefit the most from this tug-of-war. But one thing is for sure: "Online video has already shaped the course of corporate history, and now it's about to define the future, too," Fung wrote. – ***Christian Science Monitor***

_____

Earlier this month, Brett Wentworth took Level 3 Communications Inc. into territory that most rivals have been reluctant to enter. The director of global security at the largest carrier of Internet traffic cut off data from reaching a group of servers in China that his company believed was involved in an active hacking attack. The decision was reached after a broad internal review. The Broomfield, Colo., company is taking an aggressive— and some say risky approach—to battling criminal activity. Risky because hackers often hijack legitimate machines to do their dirty work, raising the risk of collateral damage by sidelining a business using the same group of servers. Such tactics also run against a widely held belief that large carriers should be facilitating traffic, not halting it. And carriers are reluctant to create the expectation that they will police the Internet.

Yet with attacks on the rise, Level 3 three years ago decided it is worth the risks. At a rate of about once every few weeks, the carrier is shutting down questionable traffic that doesn't involve any of its clients. hen the source of the trouble is hard to pinpoint, it often casts a wide net and intercepts traffic from large blocks of Internet addresses. Recently, that meant stopping traffic from a powerful network of computer servers controlled by a group of hackers that security researchers dubbed SSHPsychos. The group used rented machines in a data center to hack other computers that could bring down target websites by flooding them with junk traffic. Level 3 blocked a broad swath of the Hong Kong-registered data center's IP addresses from the Internet. "Sometimes you have to cut off a finger to save the body," Mr. Wentworth said.

Level 3 is now opening up about its methods because it wants its fellow network operators to follow its example. The stance, if copied, could change Internet carriers' traditionally passive approach to defending against attacks meant to overwhelm websites or steal vast amounts of credit card data such as have plagued U.S. retailers for the past two years. Other large Internet carriers remain wary of playing Internet cop. Swedish Internet carrier TeliaSonera AB says it usually blocks traffic when its network is under attack or its customers request it as a service. AT&T Inc. says Web traffic is often too ambiguous to block.

What may appear as a flood of Internet traffic designed to cripple a company's Web servers might actually be an unexpectedly busy day for a retailer, said AT&T Chief

Security Officer Ed Amoroso. The telecom giant focuses on attacks that target its own network or the systems of its customers and intrudes on third-party traffic only after careful discussion with its legal team. "We have to be careful, and the carrier industry has to be very careful not to go pushing buttons," Mr. Amoroso said. "You're never 100% sure of these things."

Other companies have tried more aggressive approaches against hackers in the past. Microsoft Corp. moved against botnets in 2013 when it worked with partners to cut off connections to ZeroAccess, a network of more than 2 million infected computers that their hijackers used to defraud online ad networks. Microsoft came armed in that case with a court order. Level 3 carries traffic to or from about 40% of all Internet addresses, far more than any other network, according to analysis firm Dyn Research. That means it is often hard for information sent from any website, legal or otherwise, to cross the globe without touching Level 3's equipment at some point.

The company hunts for hackers by combing through security blog posts and email advisories to get a handle on possible threats. Its software scans more than 45 billion detailed routing logs a day for signs of malicious activity before deciding to act, according to Dale Drew, Level 3's chief security officer. The security team then spends a few days studying the traffic to decide what can be ignored and what requires immediate action. More recently, the company noticed activity that appeared linked to a spate of attacks on retailers' credit card scanners with software dubbed "PoSeidon," a play on the term for point of sale machines.

Level 3 watched the attack spreading from network addresses flagged by other security experts to the criminal network's Russian and European "exfiltration servers," which collected data stolen from the infected credit card readers. Mr. Wentworth, the global security chief, watched as an employee reprogrammed Level 3's routers to misdirect the stolen data while signaling to the broader Internet that it was still on track—intentionally and covertly losing it in Level 3's network. Mr. Drew acknowledges his approach is an uphill battle. Attackers usually keep backup machines and Internet addresses handy—and that is exactly what they did in the case of PoSeidon. Minutes after Level 3 blocked the exfiltration traffic, the attackers appeared to shift to a new set of Internet addresses, forcing the carrier to quarantine even more of the Internet.

Security analysts say the credit card stealing code is still in the wild. Mr. Drew remains undeterred and plans to keep running the program as long as it sees threats worth stopping. "Everyone rationalizes why they shouldn't do anything," he said. "We're experimenting with it to see how aggressive we could be." – ***Wall Street Journal***

_____

Google Inc. showcased new offerings Thursday designed to embed the Internet giant more deeply into users' lives. At its annual developers' conference, Google unveiled a mobile-payment system to tie people closer to its Android smartphones, previewed a new operating system for connected devices, launched a service to host photos and videos on Google's computers and highlighted technology to worm itself deeper into mobile apps. "We want to make sure we leave no one behind," Google product chief Sundar Pichai told more than 1,000 developers at the I/O conference in San Francisco.

Google began in the late 1990s as a search engine harvesting information from websites and presenting relevant answers to queries. That helped build the world's largest digital advertising money machine. But the growing use of smartphones, and apps, has forced Google to adapt. Its main strategy is to extend Android from phones to as many devices as possible. Mr. Pichai said Android now runs on more than 4,000 distinct devices, from tablet computers to watches, car dashboards and TVs. "Google wants to be part of any device or service that can benefit from being smarter through technology," said Jan Dawson, an analyst at Jackdaw Research.

The approach will put Google at the heart of many products, but Mr. Dawson said it is

unclear how Google will make money from many of its new endeavors. Despite a number of announcements, there was no blockbuster new product Thursday. Google shares dipped slightly during Thursday trading, leaving them down 2% over the past year, while Apple Inc. shares have risen 50% and Facebook Inc. has gained 30%. Google shares closed down 7 cents to $554.18 Thursday.

During his keynote address, Mr. Pichai unveiled a new operating system, called Brillo, and a communication standard called Weave to connect everyday devices and objects to the Internet. Brillo is a stripped-down version of the Android mobile-operating system designed to run using little power. Weave will help devices talk to each other using a common language, so a smartphone can lock or unlock a "smart" door lock, for example. Brillo and Weave will be released by the end of 2015, Mr. Pichai said.

Google has always given away its Android operating system and tried to make money indirectly through advertising and app purchases. Jackdaw's Mr. Dawson expects that to be true for Brillo as well. Google also unveiled a new mobile-payment system called Android Pay that will let Android phone users pay with their devices in more than 700,000 U.S. stores. An updated version of Android, due to be released later this year, will support fingerprint scans for users to authenticate purchases. Google sees the service as a must-have feature for smartphones in part to keep pace with Apple's similar Apple Pay, introduced last year.

Apple takes a cut of transactions from credit-card and debit-card issuers. It is unclear how Google will get paid for Android Pay. An executive and a spokeswoman at the company said Thursday that the goal is to make Android phones more useful and declined further comment. Another potentially popular product with an unclear path to revenue emerged Thursday in Google Photos, a way of storing and organizing photos and videos in Google's data centers. Google said it will offer unlimited free storage, though large images will be compressed when stored. Van Baker, an analyst at research firm Gartner, said Photos is part of a long-term Google strategy to use its computing expertise to gather more data.

More than a decade ago, Google launched Gmail as a free email service with unlimited storage, gaining hundreds of millions of users. The company now sells ads based on the content in those messages. Mr. Baker expects Google to follow a similar approach with Photos, gaining as many users as possible, then using its computing power to analyze information and devise ways to generate revenue. "The value of the data is worth more to Google than the cost of the storage," Mr. Baker said. "They can extract activities that people like to do, places they like to go, what they like to eat."

One place Google has struggled to get information is within mobile apps, which its computers can't crawl and index like websites. Thursday, Google threw many of its most-prized assets at the challenge. The most promising example, according to Mr. Baker, was a new version of Google's digital assistant, known as Google Now. This uses the company's machine-learning capabilities and computing power to automatically suggest relevant information to users.

Google is expanding this technology to work inside mobile apps. In messaging and email apps, for example, Google Now will recommend content from other apps that are relevant to what is being discussed. App developers have to agree to have their apps indexed by Google for these features to work, a Google executive said at the conference. – *Wall Street Journal*

Broadband
Cable Association
of Pennsylvania

127 State Street, Harrisburg, PA 17101
717.214.2000 • bcapa.com

First in Broadband.
The Future of Broadband.®