Buying Verizon 5G Home is even harder than finding a Verizon mobile 5G signal

Enlarge / A Verizon 5G Home router/receiver mounted on a window.

reader comments

57 with 39 posters participating

Share this story

If you're hoping to get Verizon's 5G Home Internet service in the near future, you're probably out of luck—even if you live in one of the few cities where it's already deployed. More than two years after its unveiling, Verizon 5G Home is for sale in parts of eight cities, with an emphasis on "parts." PCMag's Sascha Segan used the 5G home service's address-lookup tool to find out how prevalent 5G Home is in areas that have Verizon 5G mobile access, and the results were disappointing.

"Since the company doesn't offer a coverage map for its home service, we pumped more than 400 Chicago and Minneapolis addresses through the Verizon 5G Home address finder and discovered that the home service has even less coverage than the mobile service does," PCMag wrote in the article published yesterday.

Segan's PCMag article includes several maps that show a large majority of houses in Verizon's 5G mobile coverage areas cannot get 5G Home. Verizon 5G mobile has limited reach to begin with because it relies on millimeter-wave frequencies that don't travel far and are easily blocked by walls. The ad

industry’s self-regulatory body recently urged Verizon to stop running ads that falsely imply the carrier’s 5G mobile service is available throughout the United States because “Verizon’s 5G coverage is primarily restricted to outdoor locations in certain neighborhoods and varies from block to block.”

Verizon 5G mobile is more prevalent in major commercial areas than on smaller residential streets, which partly explains the limited 5G Home availability. But PCMag found bad results pretty much everywhere it looked and said that the “most striking disappointment came when we looked at Chicago’s wealthy, densely populated Lakeview neighborhood. Not only did coverage not stretch beyond Verizon’s very limited mobile 5G map, addresses that appeared to be right on 5G corridors kept getting rejected.”

PCMag also recently found that AT&T’s mobile 5G is slower than its 4G in 21 out of 22 cities tested.

New equipment will help, but rollout is slow

Verizon is trying to expand 5G Home availability with an all-in-one router/receiver that it says “has a longer range from a radio standpoint so more households will be covered.” It uses a Qualcomm QTM527 antenna module. Verizon also said the new equipment can provide speeds of up to 1Gbps, although the company also promised up-to-1Gbps speeds two years ago.

Verizon urged patience with the 5G Home rollout, noting that the new hardware was just announced on Thursday last week and that the company is being conservative in bringing on new customers. Verizon’s statement to PCMag said:

> *With our new equipment, customers will have an even better 5G Home experience. Keep in mind, we’re only on day 3 with the new equipment and our new 5G Home markets. To ensure our*

> *customers have the best experience, the website is currently being a bit conservative with who is getting qualified. That said, we're expecting performance improvements and the addition of new small cells will continue to improve both coverage area and speeds.*

We asked Verizon for more detail, including the number of homes that can be served by 5G Home, and will update this article if we get a response. Besides Chicago and Minneapolis, the cities where Verizon 5G Home is available are Detroit, Sacramento, Los Angeles, Houston, Indianapolis, and St. Paul.

More than a year ago, Verizon said it plans to bring 5G Home "in due course" to every market where it deploys 5G mobile service. As of now, Verizon 5G mobile is available in parts of 36 markets. Twenty-eight of them don't have any 5G Home coverage.

Verizon 5G Home can be deployed via an antenna on a roof, requiring a visit from a Verizon technician. But typically, the service is installed by users with the receiver mounted on the inside of a window—preferably upstairs to get a better connection. "The Verizon 5G Home Internet service requires a direct line of sight between our 5G cell site and your residence," Verizon says in an FAQ. "Because of this, some residences on the same block may have the 5G Home Internet coverage, while others may not."

5G Home costs $70 a month if you don't have a Verizon Wireless mobile plan, or $50 a month if you are a mobile subscriber. While maximum download speeds are 1Gbps, Verizon says that typical download speeds are 300Mbps, and typical upload speeds are 50Mbps. 5G Home falls back to 4G LTE when a millimeter-wave signal is not available.

Slower 4G home service more widely available

Verizon also offers a 4G LTE home Internet service. The 4G service is slower than 5G Home, with advertised speeds of 25Mbps, but you have a much better chance of being able to subscribe. In a separate article, PCMag mapped out the ZIP codes where Verizon says 4G-based home Internet is at least partially available and found it has a much larger coverage area than 5G Home. That isn’t surprising because Verizon 4G relies on low- and mid-band frequencies that can cover longer distances and penetrate walls better than Verizon’s high-band spectrum.

You can check whether Verizon’s LTE Home Internet service is available at your address at this page. Verizon charges $60 a month for the LTE home service if you’re not a Verizon mobile customer, or $40 if you do have a mobile subscription. There is no monthly data cap on either the 4G or 5G home service.

https://arstechnica.com/?p=1712228

John McAfee arrested, indicted on tax evasion charges, sued for fraud

Enlarge / John McAfee gesticulating on his yacht outside Havana, Cuba, during an interview with AFP in June 2019.

reader comments

119 with 70 posters participating, including story author

Share this story

Noted cybersecurity eccentric John McAfee is under arrest in Spain awaiting extradition to the United States after being indicted on federal tax evasion charges.

The Department of Justice unsealed the indictment (PDF) yesterday following McAfee's arrest by Spanish authorities at Barcelona's airport over the weekend.

The filing alleges that McAfee deliberately not only avoided paying federal taxes from tax years 2014 through 2018 but also tried to hide considerable assets from the IRS. He allegedly hid those assets—including a yacht, a vehicle, real estate, bank accounts, and cryptocurrency—by purchasing and titling them under "the name of a nominee."

McAffee in the past has effectively dared the IRS to come get him. In 2019, he went on a Twitter screed calling taxes "illegal" and claiming he had not filed a federal tax return in eight years. "I am a prime target for the IRS," he concluded. "Here I am."

Neither the DOJ's press release nor the indictment specify how much McAfee made or owed, saying only he "earned millions" from "promoting cryptocurrencies, consulting work, speaking engagements, and selling the rights to his life story for a documentary." Another regulator, however, alleges that at least $23 million of that income came from committing fraud.

The US Securities and Exchange Commission filed a lawsuit against McAfee on Monday, alleging that he fraudulently promoted multiple initial coin offerings. According to the SEC, McAfee and his bodyguard, Jimmy Watson Jr., promoted ICOs on Twitter "pretending to be impartial and independent even

though he was paid more than $23 million in digital assets” to make those promotions.

The complaint (PDF) claims that Watson helped McAfee negotiate the payments, inflate the value of the ICOs, and cash out the payments so that McAfee profited while “investors were left holding digital assets that are now essentially worthless.” The SEC also alleges that when investors asked outright if McAfee was paid to promote those ICOs that he lied and said no, as well as making other false and misleading statements about his promotions.

If he is found guilty of the tax charges, McAfee could face up to five years in prison and a fine of $250,000 on each of the five counts of tax evasion and up to one year in prison and a fine of up to $100,000 on each of the five counts of willful failure to file a tax return, the DOJ said. The SEC suit seeks injunctive relief—i.e., a ruling banning McAfee from participating in cryptocurrency—as well as the “return of allegedly ill-gotten gains” and payment of fines.

McAfee’s wild ride

McAfee founded his eponymous computer security firm in 1987 and ran it until 1994. (Intel acquired the company in 2011, then sold it to a private equity firm in 2017.) Since departing the firm 25 years ago, he has been better known for his outlandish claims and international escapades than his software work. This is far from his first arrest.

McAfee moved to Belize in the 2000s, seemingly to avoid a wrongful death suit in the US. In 2012, authorities in Belize named him the prime suspect in the murder of another US expat. He abruptly left Belize and resurfaced in Guatemala several weeks later, where he was arrested for entering the country illegally. In 2018, a Florida court found McAfee liable for the Belize death in a wrongful death suit.

In early 2013, he resurfaced in Portland, Oregon, and claimed to have been running a massive spy network in Belize that allegedly uncovered just about every kind of scandal you can imagine. Two years later, he threw his hat into the ring for the 2016 US presidential election as a candidate for the Libertarian Party. (Gary Johnson ultimately became the Libertarian nominee.)

He also had a run-in with authorities in the Dominican Republic in 2019, when authorities detained McAfee and his wife for four days after seizing several firearms from their yacht. Dominican authorities determined the US had no active warrants or extradition requests out for McAfee at the time and so released him on his way to the UK, according to Reuters.

McAfee last spoke with Ars in 2016, discussing his offer to the FBI to personally crack the iPhone used by the deceased San Bernardino shooter in 2015. The Feds and Apple ended up in a protracted legal tangle about encryption on phones as a result of that case, an argument Attorney General Bill Barr is still pursuing.

https://arstechnica.com/?p=1712130

AT&T kills DSL, leaves tens of millions of homes without fiber Internet

Getty IMages | Synergee

reader comments

125 with 84 posters participating

Share this story

AT&T has deployed fiber-to-the-home Internet to less than 30 percent of the households in its 21-state territory, according to a new report that says AT&T has targeted wealthy, non-rural areas in its fiber upgrades.

The report, co-written by an AT&T workers union and an advocacy group, is timely, being issued just a few days after AT&T confirmed it will stop connecting new customers to its aging DSL network. That does not mean customers in DSL areas will get fiber, because AT&T last year said it was mostly done expanding its fiber service. AT&T said at the time that it would only expand fiber incrementally, in areas where it makes financial sense for AT&T to do so. We'll provide more detail on the DSL cutoff later in this article—in short, the fiber/copper hybrid known as AT&T Internet is still offered to new customers, but the slower product that AT&T sells under the DSL name is being discontinued except for existing customers.

Citing data that ISPs are required to submit to the Federal Communications Commission, the report issued today said that AT&T had built fiber-to-the-home to 28 percent of the households in its footprint as of June 30, 2019. The report was written by the Communications Workers of America (CWA), a union that represents AT&T employees; and the National Digital Inclusion Alliance (NDIA), an advocacy group that has been tracking AT&T's broadband deployments for years. The groups say that AT&T has left rural areas and people with low incomes with old, inadequate broadband services.

There are 52.97 million households in AT&T's home-Internet

service area, and 14.93 million of them have fiber-to-the-home access, the CWA told Ars. The fiber percentages were particularly bad in some states, with rates of 14 to 16 percent in Michigan, Illinois, Mississippi, and Arkansas, the CWA/NDIA report said.

“Across the predominantly rural counties in AT&T’s national footprint, only 5 percent of households (217,284 out of 4,442,675) have access to fiber,” the report said. In urban areas, the situation is better but not problem-free. “Seventy percent of households in urban counties still lack access to fiber from AT&T because the company has made fiber available to only 14.7 million households out of 48.4 million total households in these counties,” the report said.

AT&T upgrades leave poor people behind

NDIA’s research in previous years has called attention to AT&T’s “digital red-lining” in cities such as Cleveland and Detroit, in which the richest inhabitants of cities are prioritized for fiber upgrades. The new report found much the same.

“AT&T prioritizes network upgrades to wealthier areas, leaving lower-income communities with outdated technologies—households with fiber available have median income 34 percent higher than those with DSL only,” today’s report said.

AT&T can provide decent broadband speeds without building fiber all the way to each home, with a fiber-to-the-node approach that minimizes use of copper phone cables. But there are still many areas where AT&T does not offer service at the FCC’s standard of 25Mbps downstream and 3Mbps upstream. The nearly six-year-old 25/3Mbps standard has been roundly criticized by consumer advocates who say it is no longer fast enough to be considered modern broadband, but it would be a

big step up for many people in AT&T territory.

“For 28 percent of the households in its network footprint, AT&T’s Internet service does not meet the FCC’s 25/3Mbps benchmark to be considered broadband,” the CWA/NDIA report said.

Some customers in AT&T territory are lucky enough to have a cable operator that can provide modern speeds. But even for them, AT&T’s failure to deploy fiber means they “are deprived of the benefits of competition in price, choice, and service quality,” the report said. The lack of competition especially hurts people with low incomes, the report explained:

> *Without competition for market share, providers have minimal incentive to expand the market by recruiting and supporting new broadband adopters—for example, by promoting low-income discount programs or investing in community digital inclusion partnerships. NDIA’s affiliates are finding that their community members who qualify for the AT&T’s low-income discount offering, Access from AT&T, often find that the data speeds available at their homes are too slow for the video-intensive applications they need for school, work, and telemedicine.*

Cable giants Comcast and Charter have benefited from telcos like AT&T failing to upgrade tens of millions of homes to fiber services, giving the cable companies de facto monopolies in many parts of the US. AT&T has about 15.2 million Internet subscribers, compared to 29.4 million for Comcast and 28.1 million for Charter.

In mid-2015, the Federal Communications Commission required AT&T to deploy fiber to 12.5 million customers in exchange for approving its purchase of DirecTV. As the CWA/NDIA report noted, “AT&T largely halted its national build-out of fiber to residential homes in mid-2019 after it met FCC-imposed conditions following the acquisition of DirecTV.”

We contacted AT&T this morning and will update this article if we get a response.

https://arstechnica.com/?p=1711767

Botched Excel import may have caused loss of 15,841 UK COVID-19 cases

Ars Technica

reader comments

191 with 114 posters participating, including story author

Share this story

Public Health England admitted on Sunday that the agency has under-reported COVID-19 infections by 15,841 cases in recent days due to a “technical issue.” The missing positive tests were conducted between September 25 and October 2 and have since been added to national statistics, the agency said.

PHE didn’t explain the nature of the technical issue, but a number of British news sources have pointed the finger at Microsoft Excel. Here’s how the Guardian describes the issue:

> *PHE was responsible for collating the test results from public and private labs, and publishing the daily updates on case count and tests performed.*

> *In this case, the Guardian understands, one lab had sent its daily test report to PHE in the form of a CSV file – the simplest possible database format, just a list of values separated by commas. That report was then loaded into Microsoft Excel, and the new tests at the bottom were added to the main database.*
>
> *But while CSV files can be any size, Microsoft Excel files can only be 1,048,576 rows long. When a CSV file longer than that is opened, the bottom rows get cut off and are no longer displayed. That means that, once the lab had performed more than a million tests, it was only a matter of time before its reports failed to be read by PHE.*

The agency says it will take precautions to make sure an error like this doesn't happen in the future.

In addition to understating the number of COVID cases in official statistics, the glitch also hampered contact tracing efforts because data about the missing positive tests were not passed along to contact tracers. Officials stressed that the test subjects themselves got their test results as normal.

The United Kingdom is currently in the middle of a second surge in coronavirus infections. Infections in the country peaked in April and then declined to a few hundred per day in July. But cases have soared over the last month, and in recent days the UK has reported more than 10,000 new cases per day (including the previously missing cases). That's about as many as the US on a per capita basis.

Update (1:25pm): The BBC offers a different Excel-related explanation for the error:

> *PHE had set up an automatic process to pull this data together into Excel templates so that it could then be uploaded to a central system and made available to the NHS Test and Trace team as well as other government computer*

> *dashboards.*
>
> *The problem is that the PHE developers picked an old file format to do this – known as XLS.*
>
> *As a consequence, each template could handle only about 65,000 rows of data rather than the one million-plus rows that Excel is actually capable of.*
>
> *And since each test result created several rows of data, in practice it meant that each template was limited to about 1,400 cases. When that total was reached, further cases were simply left off.*

https://arstechnica.com/?p=1711742

This congressperson wants to ramp up COVID-19 testing

Enlarge / Doctor in protection gloves examining & organising test kit for COVID-19 in laboratory.
Tang Ming Tung | Getty Images

reader comments

52 with 36 posters participating

Share this story

The US’s COVID testing failure has unfurled in stages. First, there weren’t close to enough tests, thanks to cascading

policy failures and supply chain issues. Once the supply problem gradually came under control, it was replaced by processing backlogs: As cases soared over the summer, many people were having to wait a week or more to get results back. A national survey in August found that only 37 percent of people receiving nasal swab tests were getting results back in the two-day window necessary for effective contract tracing, while nearly a third of tests were taking longer than four days. This delay meant that, as Bill Gates colorfully told WIRED's Steven Levy in August, "The majority of all US tests are completely garbage." The root of the problem, Gates said, was that the federal reimbursement rate for the labs that process COVID tests is the same regardless of how long the results take. Change that, he argued, and the labs processing tests "will fix it overnight."

A new House bill would aim to make Gates' idea reality. On Thursday, Mikie Sherrill, a freshman congressperson from New Jersey, introduced the SPEEDY Act, which would tie federal reimbursement to test result speeds. (The full name is the "Strictly Pay for Efficient and Expedited Delivery of Your (SPEEDY) COVID-19 Test Act.") At the outset of the pandemic, the government was paying about $51 per test for people covered by federal health plans. (The average marginal cost of a standard PCR test varies, but at a high-volume lab it runs at about $40.) To encourage labs to increase capacity, the Centers for Medicare and Medicaid Services (CMS) raised that to $100 in April. Under the SPEEDY Act, tests that deliver results in 24 hours would be rewarded with $125; within 48 hours, the current $100 rate would apply; and for results within 72 hours, labs would go back to the pre-April reimbursement. The government wouldn't pay at all for results that come back after 72 hours. (To avoid having labs just give up on tests after that window closes, the law would require them to still process the tests in order to participate in Medicare.)

“A turnaround time of over 72 hours is pretty much useless,” said Sherrill, whose staff consulted with public health experts on the bill. Someone waiting for a negative result might be unable to return to work, missing out on a paycheck. Meanwhile, they and their contacts could be spreading the disease.

The industry is not on board with Gates’ critique or Sherrill’s proposal. “The assertion that labs would perform COVID-19 tests more quickly if they are not reimbursed for tests performed outside a specific time window is flat out wrong,” wrote Julie Khani, president of the American Clinical Laboratory Association, the trade group that includes testing giants LabCorp and Quest Diagnostics, in an emailed statement. “The proposal you describe works against our collective goal to expand testing capacity, fails to address the underlying factors affecting turnaround time and threatens access to testing for populations at the highest risk.”

Khani didn’t elaborate on what exactly would need to be addressed for faster results, but experts have variously complained about a lack of chemical reagents, lack of the expensive machines needed to read the tests, lack of staff trained to use those machines, and lack of certified lab spaces. The theory behind the SPEEDY Act is that tying payment to testing result times, and offering a bonus for extra quick turnarounds, will give labs the proper incentive to invest in those resources.

It’s hard to get a precise estimate of the extent of testing delays. There hasn’t been a national survey since August. Anecdotally, it remains trivially easy to find examples of people waiting four or five days for results. Without fast test results, tracking the spread of the virus, and by extension containing it, is impossible.

“If you’re talking about contact tracing efforts and how quickly you find people who’ve been exposed, even a day or two can be a lot,” said Emily Gurley, an infectious disease epidemiologist at Johns Hopkins Bloomberg School of Public Health. By the time most people with symptoms come in for a test, she explained, they’ve just begun infecting other people. If the test takes several days to process, those people are likely to already be infectious by the time the result comes back. Multiply this by thousands or millions and it makes the task of tracing and controlling outbreaks almost impossible. “There’s been a lot of investment in contact tracing programs—building them up and hiring people and training people—but no matter how good those programs are, if test results are late, they’re never going to be that effective.”

The law would only govern federal reimbursement, not private plans or tests purchased by state and local governments. But because Medicare and Medicaid together insure one third of Americans, and the federal government is also covering tests for the 9 percent of Americans who lack insurance, that’s nearly half the market. Meanwhile, the federal health programs shape what happens in the private sector. “Medicare ends up being how we drive many of the changes in the medical system, even for the non-Medicare patients,” said Ashish Jha, dean of the Brown University School of Public Health and one of the experts who advised on the bill. “Private payers in general don’t negotiate every single individual service. They tend to negotiate a broad package of services and they use Medicare’s payment schedule as a jumping-off point. That means whatever Medicare is paying for this test, that will also trickle down into what private insurers are paying for it.”

As with any bill introduced in a divided Congress a month before Election Day, the prospects for the SPEEDY Act to become law are uncertain. Sherrill’s two cosponsors, Suzan DelBene of Washington and Terri Sewell of Alabama, are fellow

Democrats. But she’s optimistic that she can pick up broad support and anxious to improve testing before the winter months bring a potentially devastating new virus surge.

“I think it should have a great deal of bipartisan appeal,” she said. “Making sure we have access throughout the country to testing, making sure you know the outlines of the disease—that’s kind of a cornerstone of pandemic response.”

This story originally appeared on wired.com.

https://arstechnica.com/?p=1711434

Russia’s Fancy Bear hackers likely penetrated a federal agency

Enlarge / SONY DSC
Boris SV | Getty Images

reader comments

9 with 8 posters participating

Share this story

A warning that unidentified hackers broke into an agency of the US federal government and stole its data is troubling enough. But it becomes all the more disturbing when those unidentified intruders are identified—and appear likely to be

part of a notorious team of cyberspies working in the service of Russia's military intelligence agency, the GRU.

Last week the Cybersecurity and Infrastructure Security Agency published an advisory that hackers had penetrated a US federal agency. It identified neither the attackers nor the agency, but it did detail the hackers' methods and their use of a new and unique form of malware in an operation that successfully stole target data. Now, clues uncovered by a researcher at cybersecurity firm Dragos and an FBI notification to hacking victims obtained by WIRED in July suggest a likely answer to the mystery of who was behind the intrusion: They appear to be Fancy Bear, a team of hackers working for Russia's GRU. Also known as APT28, the group has been responsible for everything from hack-and-leak operations targeting the 2016 US presidential election to a broad campaign of attempted intrusions targeting political parties, consultancies, and campaigns this year.

The clues pointing to APT28 are based in part on a notification the FBI sent to targets of a hacking campaign in May of this year, which WIRED obtained. The notification warned that APT28 was broadly targeting US networks, including government agencies and educational institutions, and listed several IP addresses they were using in their operations. Dragos researcher Joe Slowik noticed that one IP address identifying a server in Hungary used in that APT28 campaign matched an IP address listed in the CISA advisory. That would suggest that APT28 used the same Hungarian server in the intrusion described by CISA—and that at least one of the attempted intrusions described by the FBI was successful.

"Based on the infrastructure overlap, the series of behaviors associated with the event, and the general timing and targeting of the US government, this seems to be something

very similar to—if not a part of—the campaign linked to APT28 earlier this year," says Slowik, the former head of Los Alamos National Labs' Computer Emergency Response Team.

Aside from that FBI notification, Slowik also found a second infrastructure connection. A report last year from the Department of Energy warned that APT28 had probed a US government organization's network from a server in Latvia, listing that server's IP address. And that Latvian IP address, too, reappeared in the hacking operation described in the CISA advisory. Together, those matching IPs create a web of shared infrastructure that ties the operations together. "There are one-to-one overlaps in the two cases," Slowik says.

Confusingly, some of the IP addresses listed in the FBI, DOE, and CISA documents also seem to overlap with known cybercriminal operations, Slowik notes, such as Russian fraud forums and servers used by banking trojans. But he suggests that means Russia's state-sponsored hackers are most likely reusing cybercriminal infrastructure, perhaps to create deniability. WIRED reached out to CISA, as well as the FBI and DOE, but none responded to our request for comment.

Although it doesn't name APT28, CISA's advisory does detail step-by-step how the hackers carried out their intrusion inside an unidentified federal agency. The hackers had somehow obtained working usernames and passwords for multiple employees, which they used to gain entry onto the network. CISA admits it doesn't know how those credentials were obtained, but the report speculates that the attackers may have used a known vulnerability in Pulse Secure VPNs that CISA says has been exploited widely across the federal government.

The intruders then used command line tools to move among the agency's machines, before downloading a piece of custom malware. They then used that malware to access the agency's file server and move collections of files to machines the hackers controlled, compressing them into .zip files they

could more easily steal.

While CISA didn't make a sample of the hackers' custom trojan available to researchers, security researcher Costin Raiu says that the attributes of the malware matched another sample uploaded to the malware research repository VirusTotal from somewhere in the United Arab Emirates. By analyzing that sample, Raiu found that it appears to be a unique creation built from a combination of the common hacking tools Meterpreter and Cobalt Strike, but with no obvious links to known hackers and obfuscated with multiple layers of encryption. "That wrapping makes it kind of interesting," says Raiu, director of Kaspersky's global research and analysis team. "It is kind of unusual and rare in the sense that we couldn't find connections with anything else."

Even aside from their 2016 breaches of the Democratic National Committee and the Clinton campaign, Russia's APT28 hackers loom over the 2020 election. Earlier this month Microsoft warned that the group has been carrying out mass-scale, relatively simple techniques to breach election-related organizations and campaigns on both sides of the political aisle. According to Microsoft, the group has used a combination of password-spraying that tries common passwords across many users' accounts and password brute-forcing that tries many passwords against a single account.

But if APT28 is indeed the hacker group described in the CISA advisory, it's a reminder that they're also capable of more sophisticated and targeted spying operations, says John Hultquist, the director of intelligence at security firm FireEye, which didn't independently confirm Slowik's findings linking the CISA report to APT28. "They're a formidable actor, and they're still capable of getting access to sensitive areas," says Hultquist.

APT28, before its more recent hack-and-leak operations of the last few years, has a long history of espionage operations

that have targeted US, NATO, and Eastern European government and military targets. The CISA advisory, along with the DOE and FBI findings that track related APT28 hacking campaigns, all suggest that those spying operations continue today.

“It’s certainly not surprising that Russian intelligence would be trying penetrate the US government. That’s kind of what they do,” says Slowik. “But it is worth identifying that not only is such activity continuing, it’s been successful.”

This story originally appeared on wired.com.

https://arstechnica.com/?p=1711453

Publishers worry as ebooks fly off libraries’ virtual shelves

Getty Images

reader comments

24 with 24 posters participating

Share this story

Before Sarah Adler moved to Maryland last week, she used library cards from her Washington, DC, home and neighboring counties in Virginia and Maryland to read books online. The Libby app, a slick and easy-to-use service from the company

OverDrive, gave her access to millions of titles. When she moved, she picked up another card, and access to another library's e-collection, as well as a larger consortium that the library belongs to. She does almost all of her reading on her phone, through the app, catching a page or two between working on her novels and caring for her 2-year-old. With her husband also at home, she's been reading more books, mostly historical romance and literature, during the pandemic. In 2020, she estimates, she has read 150 books.

Adler buys books "rarely," she says, "which I feel bad about. As someone who hopes to be published one day, I feel bad not giving money to authors."

Borrowers like Adler are driving publishers crazy. After the pandemic closed many libraries' physical branches this spring, checkouts of ebooks are up 52 percent from the same period last year, according to OverDrive, which partners with 50,000 libraries worldwide. Hoopla, another service that connects libraries to publishers, says 439 library systems in the US and Canada have joined since March, boosting its membership by 20 percent.

Some public libraries, new to digital collections, delight in exposing their readers to a new kind of reading. The library in Archer City, Texas, population 9,000, received a grant to join OverDrive this summer. The new ebook collection "has really been wonderful," says library director Gretchen Abernathy-Kuck. "So much of the last few months has been stressful and negative." The ebooks are "something positive. It was something new."

More expensive ebooks

But the surging popularity of library ebooks also has heightened longstanding tensions between publishers, who fear that digital borrowing eats into their sales, and public librarians, who are trying to serve their communities during a once-in-a-generation crisis. Since 2011, the industry's big-five publishers—Penguin Random House, Hachette Book Group, HarperCollins, Simon and Schuster, and Macmillan—have limited library lending of ebooks, either by time—two years, for example—or number of checkouts—most often, 26 or 52 times. Readers can browse, download, join waiting lists for, and return digital library books from the comfort of their home, and the books are automatically removed from their devices at the end of the lending period.

The result: Libraries typically pay between $20 and $65 per copy—an industry average of $40, according to one recent survey—compared with the $15 an individual might pay to buy the same ebook online. Instead of owning an ebook copy forever, librarians must decide at the end of the licensing term whether to renew.

The rising demand for digital materials has prompted some librarians to shift what they buy, even as they fear shrinking budgets amid the economic downturn. A recent survey of 400 librarians in the US and Canada found that one-third are spending less on physical books, audiobooks, and DVDs, and more on digital versions since the pandemic began. Twenty-nine percent have had their budgets frozen or reduced.

But the publishers' licensing terms make it "very difficult for libraries to be able to afford ebooks," says Michelle Jeske, director of the Denver Public Library and president of the Public Library Association. "The pricing models don't work well for libraries." Between January and July, the Denver system saw 212,000 more books downloaded than the same period

last year, a 17 percent increase.

Last year, Macmillan took an additional step, limiting each library system to only a single digital copy of a new title—at half its usual price—until it had been on the market for two months. Macmillan CEO John Sargent said he worried there was too little friction in library ebook lending. “To borrow a book in [the pre-digital days] days required transportation, returning the book, and paying those pesky fines when you forgot to get them back on time,” he wrote in a letter announcing the policy. “In today’s digital world there is no such friction in the market.” Many librarians, arguing the Macmillan policy hurt large urban systems that already struggle to keep up with demand for new and noteworthy books, organized to boycott the publisher.

COVID closings

But in mid-March, days after libraries around the country began to close, Macmillan dropped the policy. “There are times in life when differences should be put aside,” Sargent wrote in a memo. A spokesperson for Macmillan declined to comment.

Librarians argue that digital lending promotes sales in the long run, by introducing readers to authors whose books they might not have bought otherwise. Research by the OverDrive-funded organization Panorama Project suggests that library book clubs, and the marketing that goes with them, boost or don’t affect sales of the same book title. This year, for example, ebook sales were up 7.6 percent through June, according to the NPD Group. The Panorama Project is conducting more thorough research on the issue.

“I think one of the things we’ll see in the postmortem of this year is that the importance of libraries is going to stand out,” says Guy LeCharles Gonzalez, the project leader for the Panorama Project. “Any publisher that gets out of 2020 not missing their budgets too much—they’re going to owe that to

libraries” (also, he says, Amazon).

Some publishers have made changes during the pandemic. Penguin Random House just extended through the end of the year a program that allows libraries to license ebooks and audiobooks for a year at half the price they usually pay. That makes it easier for a library to, say, load up on licenses for a popular bestseller and then let them go when patrons no longer demand as many copies. (A Random House spokesperson didn’t respond to a request for comment.) Many publishers have also created one-off pandemic- or social-justice-related programs, freeing up titles for newly curious readers. Some smaller publishers still allow libraries to license ebooks in perpetuity. Amazon’s publishing arm does not sell digital copies of its books to public libraries.

But the tension between libraries and publishers remains. Libraries want more flexibility, and to assure that they’ll have their collections for a long time, says Michael Blackwell, the director of St. Mary’s County Library in Maryland and the program director for the advocacy group Readers First. “Whether or not [the pandemic] is going to convince the publishers to work better with us, I don’t know,” he says. “Frankly, I am skeptical.”

At the same time, Jeske and others worry about shifting too much of their collections online, because some residents don’t have access to ebook readers, laptops, or Wi-Fi. Librarians in Denver have taken their laptop and free Wi-Fi program outside, where they hope ventilation and distance will protect everyone against the virus. They wipe down borrowed laptops between uses.

The debate has attracted attention in Washington. The House Antitrust Subcommittee last year launched an investigation of competition in the digital marketplace, and subcommittee chair Representative David Cicilline (D–Rhode Island) has met with library advocates. “The whole issue of this negotiation

[between libraries and publishers] over the last decade derives from a place where libraries have almost no rights in the digital age," says Alan Inouye, the senior director of public policy and government relations at the American Library Association. "In the longer run, there needs to be a change in the environment or in the game. That means legislation or regulation."

This story originally appeared on wired.com.

https://arstechnica.com/?p=1711429

Nikola issues copyright takedowns against critics who use rolling-truck clip

Enlarge / A 2018 Nikola video showed the Nikola One prototype rolling down a shallow hill in Utah. Nikola now says it never claimed the truck was driving under its own power.

reader comments

95 with 76 posters participating

Share this story

Nikola has issued copyright-takedown notices targeting critics on YouTube who used clips of the promotional video in which a Nikola prototype truck was seen rolling down a hill.

Nikola last month admitted that the promotional video of a

supposedly functional Nikola One electric truck moving along a highway actually consisted of the company's vehicle rolling downhill. This week, Nikola "forced the removal of several critical videos from YouTube, saying they infringed its copyright by using footage from the company," including the truck-rolling-downhill video, the Financial Times reported yesterday.

Sam Alexander is one of at least two financial commentators who had videos removed by Google subsidiary YouTube at Nikola's request. He says that four of his videos were taken down.

"The claim is from when I showed 30 seconds of their Nikola One in Motion footage, which is what they put on Twitter and it's of their Nikola One rolling down the hill," Alexander said in a YouTube video he posted Wednesday.

[embedded content]
Nikola Motors Copyright struck me.
Alexander said he believes his videos should be protected as fair use under YouTube's policies. He used the 30-second clip of the Nikola One in videos that lasted 10 minutes or more, he said. Alexander said he put the words "Source: Nikola" in the corner when he played the truck clip and played his own audio over the clip.

"I'm fairly certain it falls under fair use," he said in the video. "That being said, I'm a little nervous because [YouTube's website] says if you challenge the [copyright] strike, then be prepared to get a lawyer and it looks like these are going to go to court, and I don't have lawyer money… I'm fairly broke."

Alexander also said he wonders why he can't simply black out the 30-second portions of his videos in order to get them back online, but, he said, "I'm not even allowed access to those videos."

“Right now my main concern is that Nikola is using copyright strikes to silence their critics,” Alexander told the Financial Times. Another YouTuber named Tom Nash “was required to take down three videos that featured criticism of Nikola,” including one that used footage of the moving truck, and has appealed YouTube’s decision, the Financial Times article said.

The original rolling-truck promotional clip is still available on Nikola’s YouTube page.

Nikola, YouTube offer slightly different explanations

A Nikola statement sent to Ars and other media outlets tries to portray YouTube as the party that initiated the video-removal process. “YouTube regularly identifies copyright violations of Nikola content and shares the lists of videos with us,” a Nikola spokesperson told Ars. “Based on YouTube’s information, our initial action was to submit takedown requests to remove the content that was used without our permission. We will continue to evaluate flagged videos on a case-by-case basis.”

YouTube offered a different description, saying that Nikola simply took advantage of the Copyright Match Tool that’s available to people in the YouTube Partner Program.

“Nikola has access to our copyright match tool, which does not automatically remove any videos,” YouTube told the FT. “Users must fill out a copyright removal request form, and when doing so we remind them to consider exceptions to copyright law. Anyone who believes their reuse of a video or segment is protected by fair use can file a counter-notice.”

We asked Nikola if it has a response to YouTube’s statement, but Nikola didn’t provide any further comment.

Rightsholders must consider fair use

YouTube’s fair-use webpage acknowledged that some copyright-takedown requests target videos that appear to be examples of fair use.

“YouTube receives lots of takedown requests under copyright law asking us to remove videos that copyright owners say are infringing,” the company says. “Sometimes those requests target videos that seem like clear examples of fair use. Courts have held that rightsholders must consider fair use before they send a copyright takedown notice, so in many cases (though it’s a very small percentage of copyright takedowns overall), we ask rightsholders to confirm they’ve done this analysis.”

Nikola founder Trevor Milton resigned from his role as executive chairman after the rolling-truck revelation, and a pending Nikola deal with GM did not close as scheduled.

Nikola is involved in a legal battle with Tesla, having sued the company alleging that the Tesla Semi was a knockoff of Nikola’s own truck design. Tesla last month filed a response accusing Nikola of basing its own truck on a 2010 concept by designer Adriano Mudri. A subsequent report by the Financial Times said that Milton purchased the designs from Mudri in 2015.

https://arstechnica.com/?p=1711297

Nearly 20,000 workers have had COVID-19, Amazon admits

Enlarge / Amazon.com Inc. signage is displayed in front of a warehouse in Staten Island, New York, US, on Tuesday, March 31, 2020.

reader comments

70 with 46 posters participating

Share this story

Amazon on Thursday released high-level data on COVID-19 infection rates among its warehouse and in-store workers, saying that almost 20,000 “front-line” employees contracted COVID-19 between March 1 and mid-September.

Of 1.37 million people who worked either in Amazon distribution facilities or in Whole Foods stores during that period, 19,816—or about 1.44 percent—have had COVID-19, Amazon said. The company released the number in the context of a corporate blog post boasting of success with its mitigation measures.

“If the rate among Amazon and Whole Foods Market employees were the same as it is for the general population rate, we estimate that we would have seen 33,952 cases among our workforce,” Amazon wrote. “In reality, 19,816 employees have tested positive or been presumed positive for COVID-19—42% lower than the expected number.” The calculations do not include Prime delivery drivers, most of whom technically are not Amazon employees.

Amazon shared a state-by-state breakdown (PDF) showing where

infections per 1,000 employees stand as compared to its projections and as compared to state-level data. For most states, Amazon's case count is indeed lower than the state-level count. That said, the company is clearly having some issues with hot spots: in both West Virginia and in Minnesota, Amazon's infection rate is higher than both its projections and the community rate. The rate for Amazon workers is also higher than the state rate in New Hampshire.

Earlier reporting by Bloomberg found that one warehouse outside of Minneapolis had an infection rate more than four times higher than the rate in the surrounding community, which likely contributes to Amazon's 3.17-percent case rate in Minnesota. That media brought that number to light, however, highlights the larger problem with Amazon's handling of COVID-19: its lack of transparency.

Opacity

Amazon's release of the data follows an in-depth report NBC News published Wednesday investigating the spread of COVID-19 in Amazon's warehouses. NBC found that Amazon's "lack of transparency" made it incredibly difficult for both workers and public health officials to get any useful information about the spread of the novel coronavirus inside Amazon facilities.

The first known COVID-19 case in an Amazon facility was identified in March, when an employee at a warehouse in Queens, New York, became infected with the disease. Throughout the spring, workers complained that Amazon was not doing enough to protect employees inside distribution centers.

One employee, Chris Smalls, was fired from his job at the Staten Island warehouse in March shortly after he helped organize a walkout in protest of Amazon's handling of the coronavirus. Company leadership promptly tried to smear Smalls as "not smart or articulate" and tried to paint him as the

sole face of worker opposition. Amazon also fired three tech workers and suspended a fourth after those employees, based in the company's Seattle headquarters, voiced concerns about the company's treatment of its warehouse workers.

Employees still frustrated with the lack of clear information have tried crowdsourcing volunteer data-gathering efforts, NBC said this week, as workers are only receiving vague information from Amazon. "The texts we get distinguish between whether there was one case or multiple cases found that day, but that's as specific as it gets. You don't know whether they were on your shift or in the same section as you," one fulfillment center employee told NBC. "To my knowledge no one in my facility was even told they were close enough to a positive case to quarantine, and it's a pretty small facility, so it seems impossible that no one came into contact with one of the people who was sick," he added.

Amazon told NBC that the notifications are kept vague for privacy reasons and added that it uses camera surveillance systems to trace employees' movements for contact-tracing purposes. The company also said in its blog post that it aims to reach 50,000 tests performed per day by November, which would work out to testing about 3.6 percent of its front-line workforce every day.

Athena, a broad coalition of racial justice and workers' rights groups, called on both Amazon and public health officials to do better.

"Since March, workers and their communities have been demanding these numbers from Amazon. Workers faced retaliation, including the risk of losing their job, just for standing up for their own health and the health of their neighbors," Athena Director Dania Rajendra said. "Public officials must immediately launch investigations into Amazon and demand that the company report data on COVID-19 cases from this point forward—publicly, regularly, and truthfully. It

couldn’t be more clear that Amazon cares only about its own bottom line and that lawmakers must compel them to, at the very least, tell the truth.”

https://arstechnica.com/?p=1711245

Paying ransomware demands could land you in hot water with the feds

reader comments

104 with 68 posters participating

Share this story

Businesses, governments, and organizations that are hit by crippling ransomware attacks now have a new worry to contend with—big fines from the US Department of Treasury in the event that they pay to recover their data.

Treasury Department officials made that guidance official in an advisory published on Thursday. It warns that payments made to specific entities or to any entity in certain countries—specifically, those with a designated “sanctions nexus”—could subject the payer to financial penalties levied by the Office of Foreign Assets Control, or OFAC.

The prohibition applies not only to the group that is infected

but also to any companies or contractors the hacked group's security or insurance engages with, including those who provide insurance, digital forensics, and incident response, as well as all financial services that help facilitate or process ransom payments.

Enabling criminals

"Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims," the advisory stated. "For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data."

Under law, US persons are generally prohibited from engaging directly or indirectly in transactions with people or organizations on the OFAC's Designated Nationals and Blocked Persons List, other prohibited lists, or in Cuba, Iran, North Korea, and other countries or regions. In recent years, the Treasury Department has added several known cyber-threat groups to its designation list. They include:

To pay or not to pay?

Law enforcement officials and security consultants have generally advised against paying ransomware demands because the payments only fund and encourage new attacks. Unfortunately, paying the ransom is often the fastest and least-expensive way to recover. The City of Baltimore incurred a loss of more than $18 million after it was locked out of its IT systems. Attackers behind the ransomware had demanded

$70,000. In response, some companies claiming to offer incident-response services for ransomware attacks simply pay the attackers.

Thursday's advisory didn't say that people are prohibited in all cases from paying ransoms.

"Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

Thursday's advisory warned that there are other reasons not to pay. It further explained that the prohibitions against ransom payments are broader than many people may assume. Fines may be levied against any US person who, regardless of location, engages in a transaction that causes a non-US person to perform a prohibited action. The OFAC may also impose civil penalties based on "strict liability," a legal principle that holds the person or group liable even if they didn't know or have reason to know they were engaging with someone who's prohibited under the sanctions laws.

"As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations," the advisory stated. "This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services."

The advisory went on to say that people won’t be penalized in all cases for paying ransoms. In some cases, victims can receive a dispensation in advance for paying a ransom. In other cases, infractions may be excused or mitigated.

“Under OFAC’s Enforcement Guidelines, OFAC will also consider a company’s self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus,” officials wrote. “OFAC will also consider a company’s full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.”

Post updated to add the last two paragraphs.

https://arstechnica.com/?p=1711128