Not so IDLE hands: FBI program offers companies data protection via deception



Enlarge / The FBI’s IDLE program uses “obfuscated” data to hide real data from hackers and insider threats, making data theft harder and giving security teams a tool to spot illicit access.
Getty Images

reader comments

5 with 5 posters participating

Share this story

The Federal Bureau of Investigations is in many ways on the front lines of the fight against both cybercrime and cyber-espionage in the US. These days, the organization responds to

everything from ransomware attacks to data thefts by foreign government-sponsored hackers. But the FBI has begun to play a role in the defense of networks *before* attacks have been carried out as well, forming partnerships with some companies to help prevent the loss of critical data.

Sometimes, that involves field agents proactively contacting companies when they have information of a threat—as two FBI agents did when they caught wind of researchers trying to alert casinos of vulnerabilities they said they had found in casino kiosk systems. “We have agents in every field office spending a large amount of time going out to companies in their area of responsibility establishing relationships,” Long T. Chu, acting assistant section chief for the FBI’s Cyber Engagement and Intelligence Section, told Ars. “And this is really key right now—before there’s a problem, providing information to help these companies prepare their defenses. And we try to provide as specific information as we can.”

But the FBI is not stopping its consultative role at simply alerting companies to threats. An FBI flyer shown to Ars by a source broadly outlined a new program aimed at helping companies fight data theft “caused by an insider with illicit access (or systems administrator), or by a remote cyber actor.” The program, called IDLE (Illicit Data Loss Exploitation), does this by creating “decoy data that is used to confuse illicit… collection and end use of stolen data.” It’s a form of defensive deception—or as officials would prefer to refer to it, obfuscation—that the FBI hopes will derail all types of attackers, particularly advanced threats from outside and inside the network.

Going proactive



TLP:GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 September 2019

PIN Number
20190917-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released TLP:GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Criminals Use Social Engineering and Technical Attacks to Circumvent Multi-Factor Authentication

Summary

The FBI has observed cyber actors circumventing multi-factor

Enlarge / A recent FBI Private Industry Notification (PIN) warned of social engineering attacks targeting two-factor authentication.

In a discussion about the FBI's overall philosophy on fighting cybercrime, Chu told Ars that the FBI is "taking more of a holistic approach" these days. Instead of reacting to specific events or criminal actors, he said, "we're looking at cyber crime from a key services aspect"—aka, what are the things that cybercriminals target?—"and how that affects the entire cyber criminal ecosystem. What are the centers of gravity, what are the key services that play into that?"

In the past, the FBI got involved only when a crime was reported. But today, the new approach means playing more of a consultative role to prevent cybercrime through partnerships with both other government agencies and the private sector. "If you ever have the opportunity to go to the courtyard at FBI Headquarters, there's a quote there. 'The most effective weapon against crime is cooperation, the efforts of all law

enforcement and the support and understanding of the American people.' That can not be more true today, but it expands from beyond just law enforcement to the private sector," Chu said. "That's because we're facing one of the greatest threats that our nation has ever faced, arguably, and that's the cyber threat."

An example of that sort of outreach was visible in a case Ars reported on in March—that of the casino kiosk vendor Atrient. FBI Las Vegas field office and FBI Cyber Division agents picked up on Twitter posts about an alleged vulnerability in Atrient's infrastructure, and the agents connected the company and an affected customer with the researchers to resolve the issue (which, in Atrient's case at least, went somewhat awry). But in these situations, the FBI now also shares information it gathers from other sources, including data gathered from ongoing investigations.

Sharing happens a lot faster, Chu said, when there's a "preexisting relationship with our partners, so we know exactly who we need to call and vice versa." And information flows faster when it goes both ways. "Just as we're trying hard to get the private industry information as fast as possible, it'd be a lot more effective if we're getting information from the private industry as well," he said. Exchanging information about IP addresses, indicators of compromise, and other threat data allows the FBI to aggregate the data, "run that against our databases and all our resources, and come up with a much stronger case, so to speak, against our adversaries," Chu noted, "along with trying to attribute or identify who did it will prevent further attacks from happening."

Some information sharing takes the form of collaboration with industry information sharing and analysis centers (ISACs) and "Flash" and "Private Industry Notice" (PIN) alerts on cybercrime issues. And to build more direct relationships with companies' security executives, the FBI also offers a "CISO

Academy” for chief information security officers twice a year at the FBI Academy in Quantico, Virginia. Attendees are indoctrinated on the FBI’s investigation approaches, and they learn what kind of evidence needs to be preserved to help spur investigations forward.

But for some sectors of particular interest, the FBI is now trying to get a deeper level of collaboration going—especially with companies in the defense industry base (DIB) and other critical infrastructure industries. The FBI sees these areas as crucial industry-spanning networks, and it hopes to build a defense in-depth against cyber-espionage, intellectual property theft, and exposure of other data that could be used particularly by other nations in a way that could impact national security or the economy.
That’s precisely where IDLE comes in.

https://arstechnica.com/?p=1632381

Congress slaps robocallers with $10,000 penalty—per call



reader comments

91 with 77 posters participating

Share this story

The US Senate unanimously passed legislation Thursday that aims to end the scourge of robocalls. The TRACED Act had already passed the House of Representatives, so it’s now headed to President Donald Trump’s desk for signature.

The new legislation allows federal authorities to seize the profits of robocall operators and assess an additional penalty of up to $10,000 per call. It also pushes telephone companies to implement SHAKEN and STIR, a suite of authentication protocols that will help the fight against robocalls.

Currently, the American telephone system makes it easy for fraudsters to spoof caller-ID information on a phone call. That makes it difficult for providers to detect and block automated and fraudulent calls. SHAKEN and STIR are industry-

developed standards that use public-key cryptography to allow phone networks to authenticate calls to one another, ensuring that caller ID information is accurate.

All year, the Federal Communications Commission has been pushing phone-service providers to adopt the standard. But some companies have lagged behind, and the FCC has not yet established a hard deadline for adopting the technology.

Now Congress is setting a deadline, ordering companies with IP-based voice networks to adopt SHAKEN/STIR within 18 months. Companies with old-fashioned non-IP networks must take "reasonable measures to implement an effective call authentication framework" in the same timeframe.

That's a fairly lenient deadline. FCC Chairman Ajit Pai had urged voice providers to adopt SHAKEN/STIR by the end of 2019, and most of the larger providers were on track to meet that deadline. Some consumer groups were pushing the agency to set a hard mid-2020 deadline. The new 18-month deadline should give the laggards plenty of time to catch up.

The implementation of SHAKEN/STIR won't end robocalls on its own. The technology aims to prevent scammers from making calls with inaccurate caller-ID information. But people might find ways to make robocalls anyway. Perhaps they'll find networks that do a poor job of monitoring outgoing calls on their networks. Maybe they'll find ways to call from international numbers. Or maybe they'll find other loopholes in the system. Preventing abuse will require coordinated effort among service providers and may take years to get right.

https://arstechnica.com/?p=1635471

PoS malware skimmed convenience store customers' card data for 8 months



reader comments

64 with 54 posters participating

Share this story

US convenience store Wawa said on Thursday that it recently discovered malware that skimmed customers' payment card data at just about all of its 850 stores.

The infection began rolling out to the store's payment-processing system on March 4 and wasn't discovered until December 10, an advisory published on the company's website said. It took two more days for the malware to be fully

contained. Most locations' point-of-sale systems were affected by April 22, 2019, although the advisory said some locations may not have been affected at all.

The malware collected payment card numbers, expiration dates, and cardholder names from payment cards used at "potentially all Wawa in-store payment terminals and fuel dispensers." The advisory didn't say how many customers or cards were affected. The malware didn't access debit card PINs, credit card CVV2 numbers, or driver license data used to verify age-restricted purchases. Information processed by in-store ATMs was also not affected. The company has hired an outside forensics firm to investigate the infection.

Thursday's disclosure came after Visa issued two security alerts—one in November and another this month—warning of payment-card-skimming malware at North American gasoline pumps. Card readers at self-service fuel pumps are particularly vulnerable to skimming because they continue to read payment data from cards' magnetic stripes rather than card chips, which are much less susceptible to skimmers.

In the November advisory, Visa officials wrote:

> *The recent attacks are attributed to two sophisticated criminal groups with a history of large-scale, successful compromises against merchants in various industries. The groups gain access to the targeted merchant's network, move laterally within the network using malware toolsets, and ultimately target the merchant's POS environment to scrape payment card data. The groups also have close ties with the cybercrime underground and are able to easily monetize the accounts obtained in these attacks by selling the accounts to the top tier cybercrime underground carding shops.*

The December advisory said that two of three attacks bore the hallmarks of Fin8, an organized cybercrime group that has targeted retailers since 2016. There's no indication the Wawa

infections have any connection to the ones in the Visa advisories.

People who have used payment cards at a Wawa location should pay close attention to billing statements over the past eight months. It’s always a good idea to regularly review credit reports as well. Wawa said it will provide one year of identity-theft protection and credit monitoring from credit-reporting service Experian at no charge. Thursday’s disclosure lists other steps card holders can take.

https://arstechnica.com/?p=1635455

Dark Overlord taunted, threatened, and extorted. Now alleged member is behind bars



reader comments

32 with 25 posters participating

Share this story

Federal authorities say they have taken custody of a UK man who was a member of The Dark Overlord, a group that has taken credit for hacking into more than a dozen companies, stolen valuable data, and then demanded ransoms for its return. Stolen material included then-unreleased episodes of popular television shows and millions of patient records.

Nathan Wyatt, 39, was extradited from the United Kingdom to St. Louis, Missouri, after losing a year-long legal fight to block the transfer. Wyatt was arraigned in US District Court for the Eastern District of Missouri on Wednesday. He pleaded not guilty.

An indictment unsealed in the case alleged Wyatt participated in hacks on three healthcare providers, a medical records company, and an accounting firm. The indictment said Wyatt conspired with other members of The Dark Overlord to hack into the companies, steal their valuable data, and threaten to publish it unless they received payments in bitcoin.

Taunts

The hackers allegedly contacted executives of the hacked companies by email and SMS text messages. When hacked companies were slow to pay the ransoms, the messages often contained threats or taunts. In July 2017, a member of the group sent a text to the daughter of an owner of one of the healthcare providers. One text read: "Hi… you look peaceful… by the way did your daddy tell you he refused to pay us when we stole his company files in 4 days we will be releasing for sale thousands of patient info. Including yours…"

Prosecutors said that Wyatt registered two phone numbers used in the crimes. One number registered a VPN account and Twitter account used in the scheme. The other number sent threatening and extortionate messages to hacked parties.

The indictment made no mention of more than a dozen other hacks that matched the same mode of operation and for which the group took credit. Among them was the release of nine episodes of *Orange Is the New Black* in April 2017. At the time, the episodes were unavailable on Netflix. According to DataBreaches.net, which has extensively covered The Dark Overlord hacks, the group managed to breach Larson Studios, a post-production facility, and make off with the following TV shows or movies:

- *A Midsummer's Nightmare* – TV Movie
- *Above Suspicion* – Film
- *Bill Nye Saves the World* – TV Series
- *Breakthrough* – TV Series

- *Brockmire* – TV Series
- *Bunkd* – TV Series
- *Celebrity Apprentice (The Apprentice)* – TV Series
- *Food Fact or Fiction* – TV Series
- *Handsome* – Film
- *Hopefuls* – TV Series
- *Hum* – Short
- *It's Always Sunny in Philadelphia* – TV Series
- Jason Alexander Project – TV Series
- Liza Koshy Special – YoutubeRed
- *Lucha Underground* – TV Series
- *Lucky Roll* – TV Series
- *Making History* – TV Series
- *Man Seeking Woman* – TV Series
- *Max and Shred* – TV Series
- *Mega Park* – TV Series
- *NCIS Los Angeles* – TV Series
- *New Girl* – TV Series

DataBreaches.net reported that The Dark Overlord was behind hacks on more than a dozen other companies, including ABC Networks, an insurance firm, a plastic surgery clinic, the maker of Gorilla Glue, a real estate company, and a human resources firm, to name just a few.

Threats

The Daily Beast reported in late 2017 that members of The Dark Overlord sent texts to parents in Iowa threatening to kill their kids. The Courier Journal reported death threats made to middle and high schools in the name of The Dark Overlord.

Last year, according to Bleeping Computer, authorities in Serbia arrested another alleged member of The Dark Overlord. The suspect was identified only by initials, making it hard to track the outcome of the arrest.

Wyatt was reportedly arrested in 2016 in connection to the

theft of intimate and nude photos from the iCloud account of Pippa Middleton, sister of Kate Middleton, the Duchess of Cambridge. He was eventually released with no charges filed. In 2017, according to DataBreaches.net, Wyatt pleaded guilty to 20 counts of fraud by false representation, two counts of blackmail, and one count of possession of an identity document with intent to deceive (a false passport).

In January, while in custody in the UK, prosecutors unearthed evidence that Wyatt was involved in extortions carried out by The Dark Overlord. He has been fighting extradition ever since.

https://arstechnica.com/?p=1635347

Contractor admits planting logic bombs in his software to ensure he'd get new work



Getty Images | ullstein bild

reader comments

40 with 28 posters participating

Share this story

Many IT workers worry their positions will become obsolete as changes in hardware, software, and computing tasks outstrip their skills. A former contractor for Siemens concocted a remedy for that—plant logic bombs in projects he designed that caused them to periodically malfunction. Then wait for a call to come fix things.

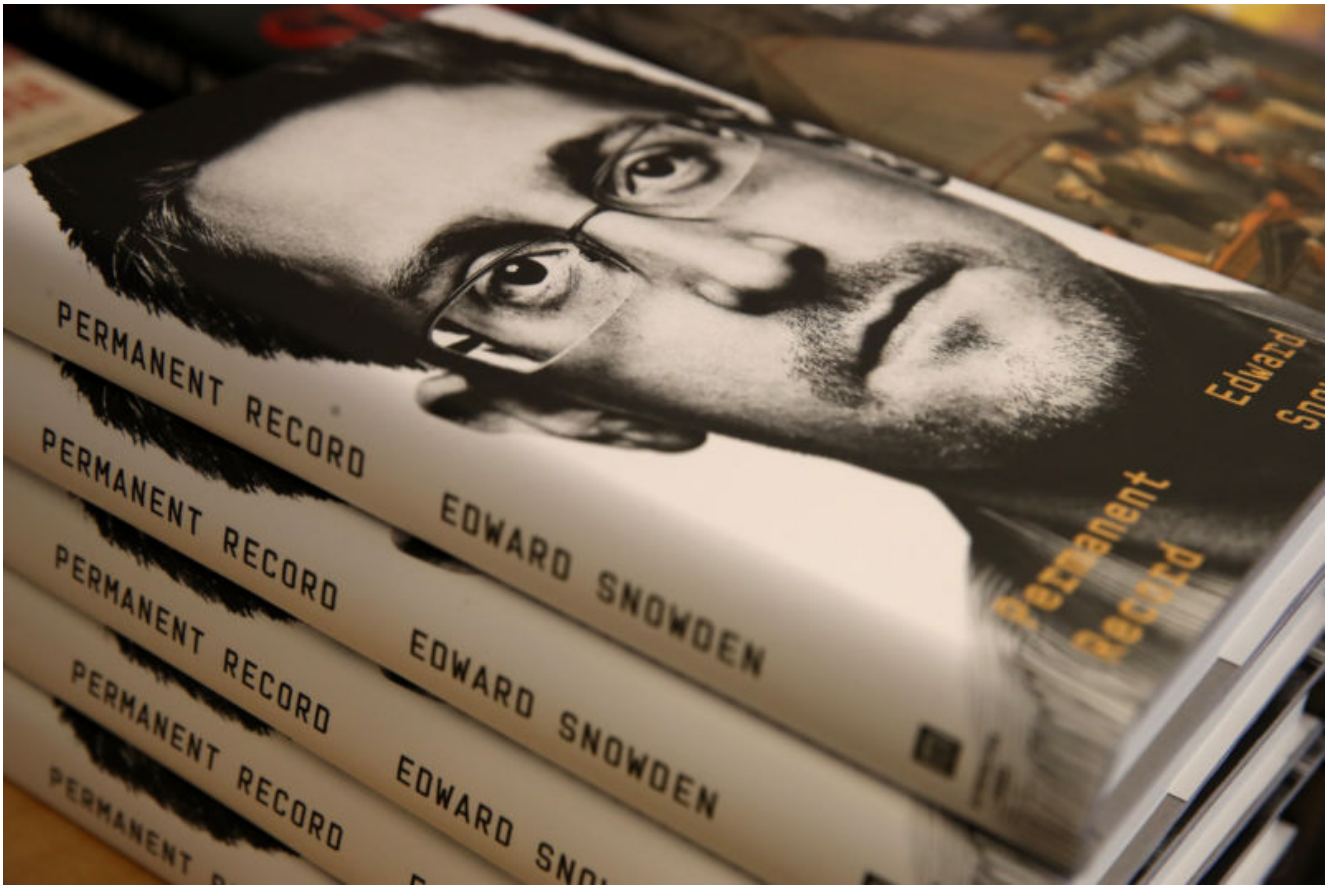
On Monday, David A. Tinley, a 62-year-old from Harrison City, Pennsylvania, was sentenced to six months in prison and a fine of $7,500 in the scheme. The sentence came five months after he pleaded guilty to a charge of intentional damage to a protected computer. Tinley was a contract employee for Siemens Corporation at its Monroeville, Pennsylvania, location.

According to a charging document filed in US District Court for the Western District of Pennsylvania, the logic bombs Tinley surreptitiously planted into his projects caused them to malfunction after a certain preset amount of time. Because Siemens managers were unaware of the logic bombs and didn’t know the cause of the malfunctions, they would call Tinley and ask him to fix the misbehaving projects. The scheme ran from 2014 to 2016.

Tinley will be under supervised release for two years following his prison term. He will also pay restitution. The parties in the case stipulated a total loss amount of $42,262.50. Tinley faced as much as 10 years in prison and a $250,000 fine.

https://arstechnica.com/?p=1634887

US government is entitled to all Snowden book proceeds, judge rules



Justin Sullivan/Getty Images

reader comments

89 with 60 posters participating, including story author

Share this story

The US government is entitled to every cent Edward Snowden earns from publishing his memoir, *Permanent Record*, a federal judge ruled on Tuesday. During his employment at the CIA and NSA, Snowden signed contracts promising to seek pre-clearance from those agencies before publishing any book or other publication containing classified materials. If he failed to do so, the contracts said, Snowden would forfeit any proceeds to the federal government.

Snowden is still in exile in Russia, where he has been stranded since 2013. The classified documents Snowden leaked to multiple journalists that year sparked an intense debate over US surveillance practices and inspired some modest

reforms. Snowden faces near-certain prosecution for espionage if he returns to the US.

The US Department of Justice filed a lawsuit on September 17, the day Snowden's book first went on sale, seeking to seize Snowden's book profits. On Tuesday, just three months later, Judge Liam O'Grady granted the government's motion for summary judgment.

Snowden's lawyers had asked O'Grady to allow the case to move forward to the discovery phase, where each side could conduct fact-finding related to the case. They argued that more information was needed to establish whether the US government had singled Snowden out for special treatment in administering the pre-clearance process.

But O'Grady rejected that request, arguing that the contracts were clear and the key facts of the case were not in serious dispute. The contracts required Snowden to get pre-clearance, and those requirements were still in effect, the judge held. Snowden had not sought pre-clearance, yet he published a book full of classified information anyway.

The judge also ruled that Snowden had breached his contractual responsibilities by giving speeches at the TED conference and other venues. Each of these speeches included slides with materials that were marked as classified. Snowden argued that he shouldn't be held responsible for re-publishing information that was already in the public domain, but the judge rejected that argument, saying that there was no such limitation in the agreement.

"Both the CIA and NSA secrecy agreements prohibit unauthorized publication of certain information, and Permanent Record discusses those types of information," O'Grady wrote. As a result, "the government is entitled to summary judgment."

https://arstechnica.com/?p=1634827

Trump administration says employers can ban organizing via company email



Enlarge / The National Labor Relations Board (NLRB) seal hangs inside a hearing room at the headquarters in Washington, D.C.

reader comments

183 with 106 posters participating

Share this story

Employers can ban employees from using work email for personal purposes, including union organizing, the National Labor Relations Board ruled on Monday. The board's three Trump-

appointed members voted for the rule, which overturned an Obama-era rule reaching the opposite conclusion. The NLRB's lone Democratic member, Lauren McFerran, dissented from the decision.

Federal labor law protects employees' right to organize without interference from employers. That includes a limited right to engage in organizing activities in the workplace. For example, an off-duty employee has a right to distribute union literature in an employee break room or the parking lot.

Labor-rights advocates have long argued that this principle should extend to workplace email systems. They point out that email can be one of the most efficient ways for workers to contact one another and discuss workplace issues. And they note that the costs to employers from added email use is negligible.

In a 2014 decision, an Obama-appointed majority of the NLRB agreed with this logic, holding that "employee use of email for statutorily protected communications on nonworking time must presumptively be permitted by employers who have chosen to give employees access to their email systems."

But then Donald Trump got elected president and Republicans gained control over the agency. They have a different perspective on the issue.

Republicans see property rights as key

The latest ruling focuses on the casino operator Caesars Entertainment, which has broad policies prohibiting employees from using its email systems for personal use. These policies don't single out union organizing. Rather, they prohibit employees from sending "non-business information" via email or using email to solicit "for personal gain or advancement of

personal views.” The policy appears to ban employees from recruiting members for their church or bowling league as much as it bans union solicitation.

Still, labor organizers objected, arguing that this broad policy impinges on worker rights to communicate with one another about workplace issues. They pointed to the Obama-era rule protecting workers’ rights to communicate with one another via email about workplace concerns.

But the NLRB’s three-member Republican majority took the case as an opportunity to overturn that rule. For the Republican board members, employer property rights are of paramount importance in the case. Employers own their email systems, the board reasoned in its Monday decision, and they have a right to decide how it’s used.

The law merely requires that workers be given some reasonable means of communicating with one another, the board held. The law already protects the rights of workers to communicate via face-to-face conversations and the distribution of literature. That gives workers sufficient opportunities to communicate to satisfy the requirements of labor law, the board ruled. In the majority’s view, it wouldn’t be appropriate to extend those protections to email because doing so infringes on the employers’ property rights to their email systems.

The board’s lone Democrat, Lauren McFerran, dissented from the ruling, arguing that the majority had misinterpreted the law. She argued that property rights weren’t relevant to the case because Caesars had already granted its employees access to the email system.

And she pointed to other cases in which the NLRB or the courts had upheld workers’ rights to communicate about labor issues using company property. For example, workers have a right to put union stickers on their hardhats—even if the hardhats are the property of the employer. That’s because the worker

already has permission to use the hardhat, and attaching a sticker doesn’t interfere with the worker’s ability to do his or her job. The same reasoning should apply to communicating about labor issues on a company email system, McFerran argued.

https://arstechnica.com/?p=1634447

Samsung chair imprisoned and 24 others found guilty in union-busting case



Enlarge / Samsung executive Lee Sang-hoon in November 2017.

reader comments

45 with 38 posters participating

Share this story

Samsung Chairman Lee Sang-hoon yesterday was sentenced to 18 months in prison, following a South Korean court ruling that he violated labor laws with union-busting activities.

Lee “was immediately arrested in court to be sent to jail,” the Financial Times reported.

Lee’s violations came during his time as Samsung chief financial officer between 2012 and 2017; he has been chairman of the board since March 2018. Samsung VP Kang Kyung-hoon also received an 18-month prison sentence for his involvement, the Financial Times wrote. The sentences were handed down by the Seoul Central District Court.

In all, about 25 current and former Samsung executives were found guilty on similar charges of violating labor laws.

“The case largely focused on efforts by Samsung officials, including Mr. Lee, to dismantle the labor union at the company’s customer-service unit,” The Wall Street Journal wrote. “The court convicted Samsung officials on multiple charges, including gathering personal information on some union members, such as their marital status, personal finances, and mental-health histories.”

Samsung admits falling short of “society’s expectations”

Samsung released a statement today saying that the company’s “understanding and view towards labor unions in the past fell short of society’s expectations.”

As Samsung board chairman, Lee Sang-hoon “is responsible for convening quarterly board meetings and reviewing the company’s financial statements before they are sent to shareholders for a vote, among other responsibilities,” the Journal wrote.

State prosecutors found that “Samsung executives used various tactics to discourage union activities, including threatening to cut the wages of employees linked to unions and withdraw business from subcontractors who appeared union-friendly,” the Financial Times wrote.

Prosecutors also alleged that Samsung executives “clos[ed] sub-contracted firms with active unions,” used “sensitive information about union members to convince them to leave,” and “delay[ed] negotiations between labour unions and management,” a BBC article said.

The court found that anti-union activities were “masterminded by executives in the firm’s now-defunct elite strategy group” and that there were “‘countless documents’ detailing tactics to undermine union activities that were distributed to affiliates by the elite unit,” the BBC wrote.

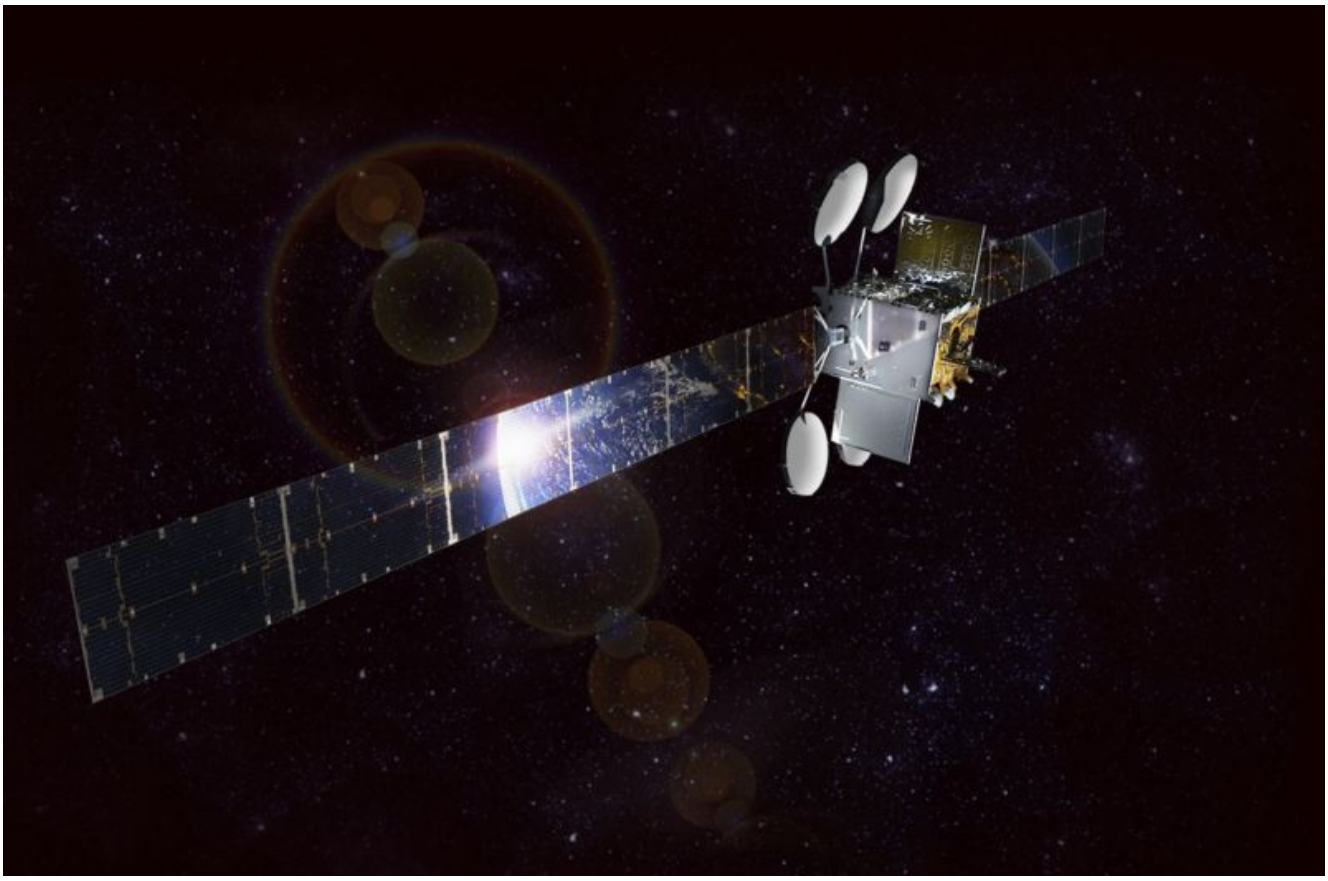
“While Lee claims there were many areas he did not know much about, [we] cannot give him immunity only due to the fact that [he] was not aware of the peripheral areas,” the judge in the case said.

Lee was indicted on the charges in September 2018.

In another case, Samsung de facto leader and Vice Chairman Lee Jae-yong was sentenced to five years in prison after being found guilty of bribery, embezzlement, hiding assets abroad, and perjury. But an appeals court in February 2018 reduced his sentence and suspended some of the charges, letting him walk free after about a year in prison. (There is no relation between Lee Jae-yong and Lee Sang-hoon.)

https://arstechnica.com/?p=1634495

No-fiber zone: FCC funds 25Mbps, data-capped satellite in rural areas



Enlarge / Viasat-2, a satellite launched by Viasat in 2017.

reader comments

68 with 54 posters participating

Share this story

The Federal Communications Commission is giving $87.1 million in rural-broadband funding to satellite operator Viasat to help the company lower prices and raise data caps.

The FCC’s Connect America Fund generally pays ISPs to expand their networks into rural areas that lack decent home Internet access. Viasat’s satellite service already provides coverage of 98 percent of the US population in 50 states, so it doesn’t need government funding to expand its network the same way that wireline operators do. But Viasat will use the money to offer Internet service “at lower cost to consumers, while also permitting higher usage allowances, than it typically provides in areas where it is not receiving Connect America Fund support,” the FCC said in its announcement yesterday.

Viasat’s $87.1 million is to be used over the next 10 years “to offer service to more than 121,700 remote and rural homes and businesses in 17 states.” Viasat must provide speeds of at least 25Mbps for downloads and 3Mbps for uploads.

While the funding for Viasat could certainly improve access for some people, the project helps illustrate how dire the broadband shortage is in rural parts of many states. Viasat’s service is generally a last-ditch option for people in areas where there’s no fiber or cable and where DSL isn’t good enough to provide a reasonably fast and stable connection. Viasat customers have to pay high prices for slow speeds and onerous data limits.

Future services relying on low-Earth-orbit satellites from companies such as SpaceX and OneWeb could dramatically boost speeds and data caps while lowering latency. But Viasat service still relies on satellites in geostationary orbits about 22,000 miles above the planet and suffer from latency of nearly 600ms, much worse than the 10ms to 20ms from fiber services (as measured in customer homes by the FCC in September 2017). Viasat’s service is classified by the FCC’s Connect America Fund as “high latency,” which is less than or equal to 750ms.

The Connect America Fund is paid for by Americans through fees on their phone bills.

Prices and data caps not revealed

A Viasat spokesperson would not tell us what prices and data caps will be applied to the company's FCC-subsidized plans. Viasat said it will provide the required 25Mbps service "along with an evolving usage allowance, and at FCC-defined prices, to certain areas, where we will be subject to a new range of federal and state regulations."

The materials released by the FCC yesterday don't provide price and data-cap information, either. We contacted the FCC and will update this article if we get any answers.

Viasat's current prices and data allotments are pretty bad, so hopefully there will be a significant improvement. Plans and pricing vary by ZIP code; offers listed on BroadbandNow include $50 a month for download speeds of up to 12Mbps and only 12GB of "priority data" each month. The price rises after a two-year contract expires.

"Once priority data is used up, speeds will be reduced to up to 1 to 5Mbps during the day and possibly below 1Mbps after 5pm," BroadbandNow's summary says. Customers can use data without affecting the limit between 3am and 6am.

Other plans include $75 a month for speeds of 12Mbps and 25GB of priority data; $100 a month for 12Mbps and 50GB; and $150 a month for 25Mbps and "unlimited" data. Even on the so-called unlimited plan, speeds "may be prioritized behind other customers during network congestion" after you use 100GB in a month. Because of these onerous limits, Viasat lowers streaming video quality to reduce data usage. Viasat says it provides speeds of up to 100Mbps but only "in select areas."

Viasat also charges installation fees, a $10-per-month equipment lease fee, and taxes and surcharges. Viasat offers a 2-year price lock, but this does not apply to the taxes and surcharges. In order to avoid signing a 2-year contract, you

have to pay a $300 “No Long-Term Contract” fee.

https://arstechnica.com/?p=1634071

Sacklers siphoned nearly $11 billion from Purdue amid opioid crisis



Enlarge / A Tufts employee removes letters from signage featuring the Sackler family name in Boston on Dec. 5, 2019. Tufts University stripped the Sackler name from buildings and programs after months-long conversations and a report that censured the school for its relationship with the family behind OxyContin, an opioid blamed for hundreds of thousands of deaths nationwide. The Sackler family gave Tufts $15

million over nearly 40 years and got its name prominently displayed throughout the university's Boston health sciences campus.

reader comments

88 with 74 posters participating

Share this story

As the epidemic of opioid abuse and overdoses ravaged the United States—claiming hundreds of thousands of lives—the Sackler family withdrew more than $10 billion from its company, OxyContin-maker Purdue Pharma. That's according to a new 350-page audit commissioned by Purdue as part of the company's Chapter 11 bankruptcy restructuring.

The revelation is likely to fuel arguments from some states that say the Sacklers should offer up more cash to settle the more than 2,800 lawsuits accusing them and Purdue of helping to spark the opioid crisis. The plaintiffs in those cases—mostly states and local governments—collectively allege that Purdue and the Sacklers used aggressive and misleading marketing to push their highly-addictive painkillers onto doctors and patients.

In a proposed $10-$12 billion settlement, the family has offered at least $3 billion of its own fortune. The family also said it would give up ownership of Purdue, which will transform itself into a public-benefit trust.

While some of the states have tentatively agreed to the deal, 24 states say that the offer isn't good enough—and that the information in the new audit proves it.

New York Attorney General Letitia James said in a statement:

> *The fact that the Sackler family removed more than $10 billion when Purdue's OxyContin was directly causing countless addictions, hundreds of thousands of deaths, and*

> *tearing apart millions of families is further reason that we must see detailed financial records showing how much the Sacklers profited from the nation's deadly opioid epidemic… We need full transparency into their total assets and must know whether they sheltered them in an effort to protect against creditors and victims.*

The audit doesn't reveal the family's total worth or where all the Purdue money ended up. But what it does reveal doesn't paint a flattering picture of the Sacklers.

Follow the money

Most strikingly, the audit shows that the family dramatically ramped up its withdrawals as the opioid epidemic raged. Between 1995 and 2007, the family withdrew just $1.3 billion from Purdue. But from 2008 to 2017, the family's withdrawals totaled $10.7 billion, peaking at $1.7 billion in 2009, as The New York Times points out.

In 2007, Purdue and three of its executives pleaded guilty in federal court to misleading regulators, doctors, and patients about the addictiveness and abuse-potential of OxyContin.

The boost in withdrawals and its timing appear to support the argument from some states that the Sacklers were trying to shield OxyContin profits from the avalanche of litigation they saw coming. As NPR notes, a briefing filed in court and signed by 25 attorneys general read:

> *The Sacklers knew that the profits were not safe inside Purdue. Richard Sackler warned, in a confidential memo, that the company posed a "dangerous concentration of risk." Purdue's CFO stated that a single lawsuit by a state attorney general could "jeopardize Purdue's long-term viability." So the Sacklers pulled the money out of the company and took it for themselves. The Sacklers have directed Purdue to pay*

their family as much as $13 billion.

Where the money ended up is still unclear. As the NYT points out, money was often directed to trusts in places considered tax havens, such as Luxembourg or the British Virgin Islands. The audit also outlined the complex way in which the family sometimes moved money around. In some cases, Purdue money moved through a series of companies, including Rosebay Medical and Beacon Co., holding companies controlled by the family. In 2017, a set of a dozen transactions moved money through several companies before finally directing it to a Japanese division of Mundipharma, the Sacklers' global pharmaceutical company. The audit does not provide an explanation for the transfers.

https://arstechnica.com/?p=1634067