BY ANDY GREENBERG AND MATT BURGES

Elon Musk SpaceX Satellites Are Leaking the World's Secrets: Calls, Texts, Military and Corporate Data

With just $800 in basic equipment, researchers found a stunning variety of data—including thousands of T-Mobile users' calls and texts and even US military communications—sent by satellites unencrypted.

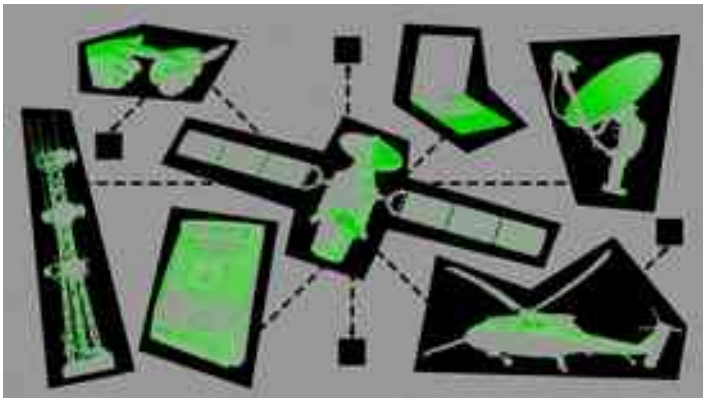


PHOTO-ILLUSTRATION: JACQUI VANLIEW; GETTY IMAGES

SATELLITES BEAM DATA down to the Earth all around us, all the time. So you might expect that those space-based radio communications would be encrypted to prevent any snoop with a satellite dish from accessing the torrent of secret information constantly raining from the sky. You would, to a surprising and troubling degree, be wrong.

Roughly half of geostationary satellite signals, many carrying sensitive consumer, corporate, and government communications, have been left entirely vulnerable to eavesdropping, a team of researchers at UC San Diego and the University of Maryland revealed today in a study that will likely resonate across the cybersecurity industry, telecom firms, and inside military and intelligence agencies worldwide.

For three years, the UCSD and UMD researchers developed and used an off-the-shelf, $800 satellite receiver system on the roof of a university building in the La Jolla seaside neighborhood of San Diego to pick up the communications of geosynchronous satellites in the small band of space visible from their Southern California vantage point. By simply pointing their dish at different satellites and spending months interpreting the obscure—but unprotected—signals they received from them, the researchers assembled an alarming collection of private data: They obtained samples of the contents of Americans' calls and text messages on T-Mobile's cellular network, data from airline passengers' in-flight Wi-Fi browsing, communications to and from critical infrastructure such as electric utilities and offshore oil and gas platforms, and even US and Mexican military and law enforcement communications that revealed the locations of personnel, equipment, and facilities.

"It just completely shocked us. There are some really critical pieces of our infrastructure relying on this satellite ecosystem, and our suspicion was that it would all be encrypted," says Aaron Schulman, a UCSD professor who co-led the research. "And just time and time again, every time we found something new, it wasn't."

The group's paper, which they're presenting this week at an Association for Computing Machinery conference in Taiwan, is titled "Don't Look Up"—a reference to the 2021 film of that title but also a phrase the researchers say describes the apparent cybersecurity strategy of the global satellite communications system. "They assumed that no one was ever going to check and scan all these satellites and see what was out there. That was

their method of security," Schulman says. "They just really didn't think anyone would look up."

The researchers say that they've spent nearly the past year warning companies and agencies whose sensitive data they found exposed in satellite communications. Most of them, including T-Mobile, moved quickly to encrypt those communications and protect the data. Others, including some owners of vulnerable US critical infrastructure whom the researchers alerted more recently—and declined to name to WIRED—have yet to add encryption to their satellite-based systems. Researchers have pointed to the surveillance dangers of unencrypted satellite connections before, but the scale and scope of the new disclosures appear unrivaled.

BY GREGORY BARBER

UCSD and UMD researchers pose with their satellite receiver system on the roof of a university building in San Diego. From left to right: Annie Dai, Aaron Schulman, Keegan Ryan, Nadia Heninger, Morty Zhang. Not pictured: Dave Levin.

COURTESY OF RYAN KOSTA

The researchers' work looked at only a small fraction of geostationary satellites whose signals they could pick up from San Diego—roughly 15 percent of those in operation, by the researchers' estimate. This suggests vast amounts of data are likely still being exposed over satellite communications, says Matt Green, a computer science professor at Johns Hopkins University who focuses on cybersecurity and reviewed the study. Large swaths of satellite data will likely be vulnerable for years to come, too, as companies and governments grapple with whether and how to secure outdated systems, Green says.

"It's crazy. The fact that this much data is going over satellites that anyone can pick up with an antenna is just incredible," Green says. "This paper will fix a very small part of the problem, but I think a lot of it is not going to change."

GEAR NEWS AND EVENTS

New Rules Could Force Tesla to Redesign Its Door Handles. That's Harder Than It Sounds

BY AARIAN MARSHALL

DIGITAL CULTURE

The 'Womanosphere' Is Reshaping the Conservative Dating Landscape

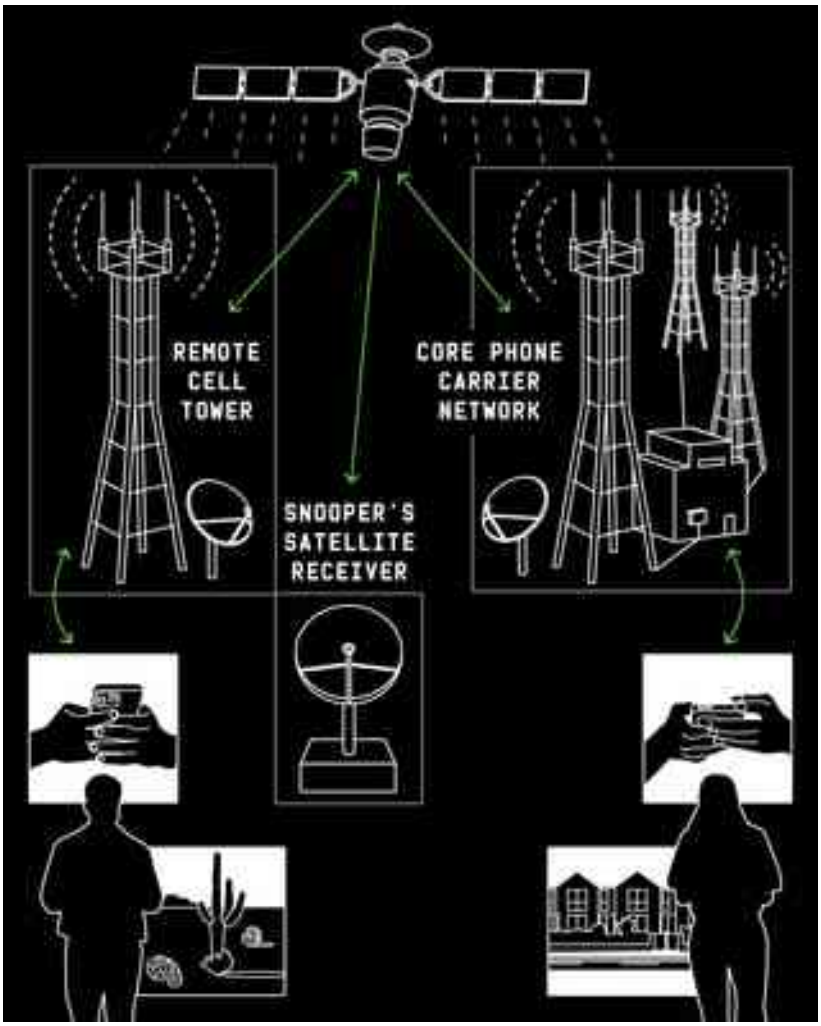
"I would be shocked," Green adds, "if this is something that intelligence agencies of any size are not already exploiting."

Half Conversations, Broadcast From Space

The phone calls and text messages the researchers obtained, in particular, were exposed due to telecoms' often overlooked use of satellite communications for offering cellular coverage to normal phone users who connect to cell towers in remote locations. Some towers in desert or mountainous regions of the US, for instance, connect to a satellite that relays their signals to and from the rest of a telecom's core cellular network, the internal communications of the network known as "backhaul" traffic.

Anyone who sets up their own satellite receiver in the same broad region as one of those remote cell towers—often as far as thousands of miles away—can pick up the same signals meant for that tower. Doing so allowed the research team to obtain at least some amount of unencrypted backhaul data from the carriers T-Mobile, AT&T Mexico, and Telmex.

The T-Mobile data was particularly significant: In just nine hours of recording T-Mobile backhaul satellite communications from their single dish, the researchers collected the phone numbers of more than 2,700 users as well as all the phone calls and text messages the researchers received during that time. They could, however, only read or hear one side of those conversations: the content of the messages and calls sent *to* T-Mobile's remote towers, not sent *from* them to the core cell network, which would have required another satellite dish near the one T-Mobile intended to receive the signal on the other end.



Cellular towers in remote regions sometimes connect to a satellite that relays their signals to and from the rest of a telecom's core cellular network—the internal communications of the network known as "backhaul" traffic. Anyone who sets up their own satellite receiver in the same broad region as one of those remote cell towers—often as far as thousands of miles away—can pick up the same signals meant for that tower.

ILLUSTRATION: WIRED STAFF; GETTY IMAGES

MOST POPULAR

SCIENCE

A New Algorithm Makes It Faster to Find the Shortest Paths

BY BEN BRUBAKER

GEAR NEWS AND EVENTS

New Rules Could Force Tesla to Redesign Its Door Handles. That's Harder Than It Sounds

BY AARIAN MARSHALL

DIGITAL CULTURE

The 'Womanosphere' Is Reshaping the Conservative Dating Landscape

BY JASON PARHAM

COMPUTERS AND SOFTWARE

Programming in Assembly Is Brutal, Beautiful, and Maybe Even a Path to Better AI

BY GREGORY BARBER

"When we saw all this, my first question was, did we just commit a felony? Did we just wiretap?" says Dave Levin, a University of Maryland computer science professor who co-led the study. In fact, he says, the team didn't actively intercept any communications, only passively listened to what was being sent to their receiver dish. "These signals are just being broadcast to over 40 percent of the Earth at any point in time," Levin says.

Mexican telecom Telmex also transmitted unencrypted voice calls, the researchers found. The researchers further discovered that AT&T Mexico transmitted raw data over satellites that included users' internet traffic—most of which was encrypted with HTTPS by the apps or browsers they used—but also some calling and texting metadata. They also found decryption keys that the researchers believe could likely have been used to decipher other sensitive information the AT&T Mexico network transmitted—though they didn't attempt this.

Starting in December 2024, the researchers began contacting the affected telecoms. T-Mobile responded by encrypting its satellite transmissions within weeks, but responses from other cell carriers were mixed.

"Last year, this research helped surface a vendor's encryption issue found in a limited number of satellite backhaul transmissions from a very small number of cell sites, which was quickly fixed," a T-Mobile spokesperson says, adding the issue was "not network-wide" and that the company has taken steps to "make sure this doesn't happen again."

A spokesperson for AT&T says the company "promptly" fixed the issue. "A satellite vendor misconfigured a small number of cell towers in a remote region of Mexico," they say. Telmex did not respond to WIRED's request for comment.

Whether other cellular carriers around the US and world—outside the visibility of the researchers' satellite dish—have encrypted their satellite-based network backhaul data remains an open question. The researchers say they didn't see any unencrypted Verizon or AT&T US traffic from their dish.

SCIENCE

A New Algorithm Makes It Faster to Find the Shortest Paths

BY BEN BRUBAKER

GEAR NEWS AND EVENTS

New Rules Could Force Tesla to Redesign Its Door Handles. That's Harder Than It Sounds

BY AARIAN MARSHALL

DIGITAL CULTURE

The 'Womanosphere' Is Reshaping the Conservative Dating Landscape

BY JASON PARHAM

COMPUTERS AND SOFTWARE

Programming in Assembly Is Brutal, Beautiful, and Maybe Even a Path to Better AI

BY GREGORY BARBER

The AT&T spokesperson says that its US and Mexico networks are separate, and it is "rare" to use satellites for cellular backhaul. "We typically route traffic on our closed, secure backhaul network," the spokesperson says. "On those rare instances where data must be transmitted outside our closed network, it is our policy to encrypt it." Verizon did not respond to WIRED's request for comment.

Beyond just cell towers in remote locations, it's possible that a lack of encryption for cellular backhaul data could make anyone on the same network vulnerable, points out Johns Hopkins' Green. Hackers might be

able to perform a so-called relay attack with a spoofed cell tower—using the surveillance hardware sometimes called a stingray or IMSI catcher—and route any victim's data to a cell tower that connects to a satellite uplink. "The implications of this aren't just that some poor guy in the desert is using his cell phone tower with an unencrypted backhaul," says Green. "You could potentially turn this into an attack on anybody, anywhere in the country."

Military Helicopters and Power Grids, Exposed

The researchers' satellite dish also pulled down a significant collection of unprotected military and law enforcement communications. They obtained, for instance, unencrypted internet communications from US military sea vessels, as well as the vessels' names. (A spokesperson for the US Defense Information Systems Agency acknowledged WIRED's request for comment but had not provided a response at the time of writing).

For Mexican military and law enforcement, the exposures were far worse: The researchers say they found what appeared to be unencrypted communications with remote command centers, surveillance facilities, and units of the Mexican military and law enforcement. In some cases, they saw the unprotected transmission of sensitive intelligence information on activities like narcotics trafficking. In others, they found military asset tracking and maintenance records for aircraft like Mil Mi-17 and UH-60 Black Hawk helicopters, sea vessels, and armored vehicles, as well as their locations and mission details. "When we started seeing military helicopters, it wasn't necessarily the sheer volume of data, but the extreme sensitivity of that data that concerned us," says Schulman. The

Mexican military did not immediately respond to WIRED's requests for comment.

MOST POPULAR

SCIENCE

A New Algorithm Makes It Faster to Find the Shortest Paths

BY BEN BRUBAKER

GEAR NEWS AND EVENTS

New Rules Could Force Tesla to Redesign Its Door Handles. That's Harder Than It Sounds

BY AARIAN MARSHALL

DIGITAL CULTURE

The 'Womanosphere' Is Reshaping the Conservative Dating Landscape

BY JASON PARHAM

COMPUTERS AND SOFTWARE

Programming in Assembly Is Brutal, Beautiful, and Maybe Even a Path to Better AI

BY GREGORY BARBER

Just as sensitive, perhaps, were industrial systems communications from critical infrastructure like power grids and offshore oil and gas platforms. In one case, they found that the Comisión Federal de Electricidad (CFE), Mexico's state-owned electric utility with nearly 50 million customers, was

transmitting its internal communications in the clear—everything from work orders that included customers' names and addresses to communications about equipment failures and safety hazards. (A CFE spokesperson acknowledged WIRED's request for comment but didn't provide a response before publication.)
In other cases they have yet to publicly detail, the researchers say they also warned US infrastructure owners about unencrypted satellite communications for industrial control system software. In their phone calls with those infrastructure owners, some owners even expressed concerns that a malicious actor might have the ability to not only surveil the control systems of their facilities, but also, with enough sophistication, potentially disable or spoof them to tamper with the facility's operation.

The researchers obtained a vast grab bag of other miscellaneous corporate and consumer data: They pulled down in-flight Wi-Fi data for Intelsat and Panasonic systems used by 10 different airlines. Within that data, they found unencrypted metadata about users' browsing activities and even the unencrypted audio of the news programs and sports games being broadcast to them. They also obtained corporate emails and inventory records of Walmart's Mexican subsidiary, satellite communications to ATMs managed by Santander Mexico, as well as the Mexican banks Banjercito and Banorte.

A spokesperson for Panasonic Avionics Corporation said they "welcome the findings" from the researchers, but claim it "has found that several statements attributed to us are either inaccurate or misrepresent our position." When asked, the spokesperson did not specify what the company considered was inaccurate. "Our satellite communications systems are designed so that every user data session follows established security protocols," the spokesperson says.

“Generally, our users choose the encryption that they apply to their communications to suit their specific application or need,” says a spokesperson for SES, the parent company of Intelsat. “For SES’s inflight customers, for example, SES provides a public Wi-Fi hot spot connection similar to the public internet available at a coffee shop or hotel. On such public networks, user traffic would be encrypted when accessing a website via HTTPS/TLS or communicating using a virtual private network.” The researchers reported the swaths of unencrypted satellite communications from the Mexican government and Mexican organizations to CERT-MX, the country’s incident response team, which is part of the government’s National Guard, in April this year, before separately contacting companies. CERT-MX did not respond to WIRED’s repeated requests for comment.

A spokesperson for Santander Mexico says that no customer information or transactions were compromised, but confirmed that the exposed traffic was linked to a “small group” of ATMs used in remote areas of Mexico where using satellite connections is the only option available. “Although this traffic does not pose a risk to our customers, we took the report as an opportunity for improvement, implementing measures that reinforce the confidentiality of technical traffic circulating through these links,” the spokesperson says.

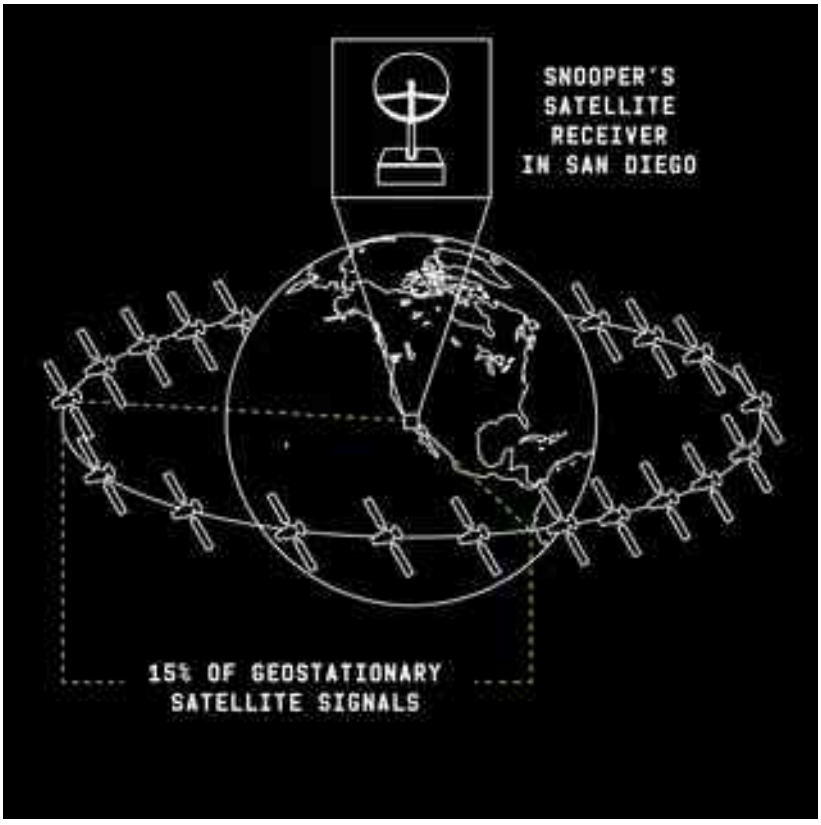
“While we cannot share specifics, we can confirm that our communications lines have been evaluated and confirmed secure,” a spokesperson for Walmart says. (The researchers confirm that they observed Walmart had encrypted its satellite communications in response to their warning.)

“The information of our customers and infrastructure is not exposed to any vulnerability,” a spokesperson for Grupo Financiero Banorte says. Banjercito could not be reached for comment.

“SIA and its members remain diligent in monitoring the threat landscape and continue to participate in various security efforts with government agencies, industry working groups, and international standards bodies,” says Tom Stroup, the president of the Satellite Industry Association, adding that it does not comment on specific company issues.

Time to Look Up

The amount of Mexico-related data in the researchers’ findings is, of course, no coincidence. Although their satellite dish was technically able to pick up transmissions from around a quarter of the sky, much of that swath included the Pacific Ocean, which has relatively few satellites above it, and only a small fraction of the transponders on the satellites it did see were transmitting data in the direction of its dish. The result, the researchers estimate, was that they examined only 15 percent of global satellite transponder communications, mostly in the western US and Mexico.



Geostationary satellites ring the Earth's equator. The researchers' satellite dish on the roof of their UC San Diego building was in a position to pick at least some signals from about a quarter of that ring. But because many of the satellites' signals weren't transmitted towards San Diego—and a large part of their coverage was over the Pacific Ocean, with relatively few satellites—they only received an estimated 15 percent of all geostationary satellite signals. That also means that other dishes placed elsewhere in the world would likely find entirely different signals transmitting different sensitive data.

ILLUSTRATION: WIRED STAFF; GETTY IMAGES

New Rules Could Force Tesla to Redesign Its Door Handles. That's Harder Than It Sounds

BY AARIAN MARSHALL

- 
  DIGITAL CULTURE

The 'Womanosphere' Is Reshaping the Conservative Dating Landscape

BY JASON PARHAM

- 
  COMPUTERS AND SOFTWARE

Programming in Assembly Is Brutal, Beautiful, and Maybe Even a Path to Better AI

BY GREGORY BARBER

That suggests anyone could set up similar hardware somewhere else in the world and likely obtain their own collection of sensitive information. After all, the researchers restricted their experiment to only off-the-shelf satellite hardware: a $185 satellite dish, a $140 roof mount with a $195 motor, and a $230 tuner card, totaling less than $800.

"This was not NSA-level resources. This was DirecTV-user-level resources. The barrier to entry for this sort of attack is extremely low," says Matt Blaze, a computer scientist and cryptographer at Georgetown University and law professor at Georgetown Law. "By the week after next, we will have hundreds or perhaps thousands of people, many of whom won't tell us what they're doing, replicating this work and seeing what they can find up there in the sky."

One of the only barriers to replicating their work, the researchers say, would likely be the hundreds of hours they spent on the roof adjusting their satellite. As for the in-depth, highly technical analysis of obscure data protocols they obtained, that may now be easier to replicate, too: The

researchers are releasing their own open-source software tool for interpreting satellite data, also titled “Don’t Look Up,” on Github.

The researchers’ work may, they acknowledge, enable others with less benevolent intentions to pull the same highly sensitive data from space. But they argue it will also push more of the owners of that satellite communications data to encrypt that data, to protect themselves and their customers. “As long as we’re on the side of finding things that are insecure and securing them, we feel very good about it,” says Schulman.

There’s little doubt, they say, that intelligence agencies with vastly superior satellite receiver hardware have been analyzing the same unencrypted data for years. In fact, they point out that the US National Security Agency warned in a 2022 security advisory about the lack of encryption for satellite communications. At the same time, they assume that the NSA—and every other intelligence agency from Russia to China—has set up satellite dishes around the world to exploit that same lack of protection. (The NSA did not respond to WIRED’s request for comment).

“If they aren't already doing this,” jokes UCSD cryptography professor Nadia Heninger, who co-led the study, “then where are my tax dollars going?”

Heninger compares their study’s revelation—the sheer scale of the unprotected satellite data available for the taking—to some of the revelations of Edward Snowden that showed how the NSA and Britain’s GCHQ were obtaining telecom and internet data on an enormous scale, often by secretly tapping directly into communications infrastructure.

“The threat model that everybody had in mind was that we need to be encrypting everything, because there are governments that are tapping undersea fiber optic cables or coercing telecom companies into letting

them have access to the data," Heninger says. "And now what we're seeing is, this same kind of data is just being broadcast to a large fraction of the planet."

Andy Greenberg is a senior writer for WIRED covering hacking, cybersecurity, and surveillance. He's the author of the books *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency* and *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. His books ... Read More

SENIOR WRITER

Matt Burgess is a senior writer at WIRED focused on information security, privacy, and data regulation in Europe. He graduated from the University of Sheffield with a degree in journalism and now lives in London. Send tips to Matt_Burgess@wired.com. ... Read More

SENIOR WRITER