You ever think about the proliferation of weapons?
Well, shoot, let's get into it.
I want you to think about this guy, Sam Cummings.
Here, I found an old vintage documentary made by CNN.
This is Sam Cummings, and this 57-year-old is the biggest
private military weapons dealer in the world.
The business as a business is fascinating.
Cummings has sold tens of millions of guns to armies and sportsmen.
OK, so how did he become the biggest private military weapons
dealer in the world?
Well, the U.S. Department of Defense taught him.
That's how.
When he was 18 in 1945, he was recruited into the U.S.
Army, which at the time they were just wrapping up World War Two.
There was a big ramp up to provide all these weapons for armies
around the world to use in wars.
And then suddenly the war was over.
So where's all the weapons going to go?
As a young arms buff, Cummings got his start at the CIA.
His assignment was to buy surplus weapons in Europe.
At the age of 23, he left the spy agency and started his own business.
Buying surplus weapons in the CIA gave him a crazy idea.
How about buy a whole bunch of cheap weapons now that the war is over
and then slowly sell them over time?
He had all the contacts he needed to go buy them.
And so he did.
And he was selling them to the public.
Like to hunters or sportsmen and was becoming known for having a big supply of weapons.
But he wanted bigger deals.
And so he started talking to governments around the world.
He brought a bunch of AR-10 rifles down to Nicaragua and demonstrated that to them there.
Well, the Nicaraguan military was like, ah, that's cool.
Send us some of those.
And then the Dominican Republic wanted some and then Cuba wanted some.
And yet he sold battle rifles to all these places, including Fidel Castro.
Which I think was illegal because it was an embargo not to sell any weapons to Castro.
Yet it still happened.
Fidel Castro bought rifles from him and he did not seem to get in any trouble for that.
I don't think he cared who he sold to.
If you had money, he'd sell you weapons.
Every morning, Cummings uses a Telex to keep in touch with his military customers and branch offices.
A Telex comes in from Sudan, offering surplus military equipment.
I would go about 25% more than that in dollars if my list is the same as your last.

Cummings military weapons are shipped and stored at Interarm's house in Manchester, England.
At any given moment, there are a quarter of a million guns here.
And on little notice, Cummings says he would have no trouble equipping a fair-sized army.
Depends how large the army would be, but let's say an army of an average smaller African or Latin American state is
25 to 50,000 men. No problem.
Can you believe this kind of thing was going on in the 50s and 60s?
Sam Cummings has sold or bought arms from almost every country in the world.
Interarm's has supplied Africa and his company's weapons have shown up in Egypt.
His guns were used at the Bay of Pigs by Fidel Castro and in Nicaragua under Samosa.
The Cummings best customers are countries in Asia.
This guy became a billionaire, selling hundreds of thousands of weapons to anyone who would pay.
And a lot of time, you would buy these weapons from Russia, which was in the middle of a cold war with the US.
I would say the Russians build the best military weapons across the board, and they also build them in tremendous quantity,
which is the key factor in modern war.
I don't know. I feel like this guy's only ally in life is money.
He doesn't mind selling weapons to places that are actively at war with his home country, you know?
So clearly he doesn't have an allegiance to the US.
And from watching this documentary, he seems to believe that all sides are evil and there's just no way to take the moral high ground on any of these trade deals.
He does seem to have some kind of allegiance to his family, though.
He invited this CNN reporter on an eight hour car ride where they were going on a family trip somewhere.
And I think it's pretty weird to have a reporter in the car with the whole family for eight hours.
But okay.
He asked us not to take pictures of his wife or his college age daughters for security reasons.
Well, strangely enough, years later, one of those daughters, Susan, killed her boyfriend by shooting him four times and was convicted and had to serve prison time.
These are true stories from the dark side of the internet.
I'm Jack Reciter.
This is Dark Net Diaries.
This episode is sponsored by Linode, which is now Akamai, and this is exciting news for developers.
Linode is now part of Akamai Connected Cloud, the massively distributed edge and cloud platform that puts apps and experiences closer to the users and keeps threats farther away.
Increased performance and speed to market with cloud computing services you're used to, now running on the Akamai Connected Cloud.
All the developer friendly tools that have helped you build on Linode for the past two decades are still available now that Linode is part of Akamai.
In fact, they're expanding their services to offer even more cloud computing resources and tools while providing reliable, affordable and scalable solutions for businesses of all sizes.
As part of Akamai's global network, they're also expanding data centers worldwide, giving you access to even more resources to help you grow and serve your users.

Experience the power of Akamai Connected Cloud for yourself and see why developers worldwide choose it for their cloud computing needs.
Learn more at akamai.com or linode.com that's spelled A-K-A-M-A-I dot com or linode is spelled L-I-N-O-D-E dot com.
Support for this episode comes from Exonius.
Complexity is increasing in IT and cybersecurity.
Adapt to the demands of your modern environment with Exonius and say goodbye to manual asset inventory approaches.
The Exonius solution provides an always up-to-date inventory, uncovers gaps and automates action, giving you the solid foundation you need to stay dynamic in the face of complexity.
Go to exonius.com slash darknet to learn more and get a demo that's spelled A-X-O-N-I-U-S exonius.com slash darknet.
All right, so let's start out with what's your name and what do you do?
I'm Croft and Black.
I'm a reporter at Lighthouse Reports.
Lighthouse Reports is an investigative non-profit working with some of the world's leading media companies on topics like migration and surveillance.
And a lot of episodes you hear on my show are sometimes slapped together in a matter of weeks and it's just me doing the research, but not this episode.
Here, we have the luxury of talking with a real reporter who spent lots of time on this story.
Well, this article was like a big team effort, right?
Because, I mean, first of all, we at Lighthouse, we wouldn't have got involved in it without the work that Inside Story and Grease did.
And for me personally, working with those guys was just a huge privilege because they're so knowledgeable and so capable and the material they were able to dig up was truly astounding in some cases.
And, you know, I guess for me, it was cool because, you know, I'm a plain tracking guy for a long time and, you know, I got into this business as a, you know, doing plain tracking stuff when I was tracking CIA rendition flights.
So, you know, for me, it was kind of funny to do a story that combined those two things.
That's never happened before and I wonder if it'll ever happen again.
So yeah, that got a personal space in my heart for this story, for that reason, really.
The team at Lighthouse Reports spent over six months researching this story and they worked together with other reporters and journalists and researchers, places like Inside Story and Grease and Haaretz in Israel.
They published similar stories too.
And when I first read the story, I was like, whoa, what?
So buckle up and let's go for a ride.
The person at the center of the story is a guy named Tal Dillion.
Tal's an Israeli entrepreneur, a long time guy in the cyber business, formerly in the military, like a lot of those guys are, came out and he was involved in a very famous phone geolocation outfit called Circles back in the day.
So I want to jump in here and underline this for a second.
Tal went through the Israeli military.

Specifically, he was in Unit 81, which designs new tools for the Israeli military to use.
I've heard that Unit 81 once designed a little microphone that is supposed to look like a rock.
So you could just set it down in an area you want to record audio in and it's hidden so nobody knows they're being recorded.
I imagine they make a lot of spy gear for the Israeli military.
Yeah, so Tal came out of that division and when he left the military, he created a company called Circles, which I believe was a surveillance company that used SS7 attacks to spy on mobile users.
SS7 attacks are really fascinating.
I'm not going to get bogged down into the details of how they work, but real quick, SS7 is a way to exploit mobile carriers into getting info on the users or even taking over their phone number.
And I believe this company that Tal started, Circles, was using SS7 attacks to collect data from targets and intercept messages and phone calls.
Well, this became quite the service.
So much so that NSO group was like, Hey, that's cool.
Can we buy it?
Now, NSO group is someone I've covered in detail before.
That's episode 100.
And it's actually the most listened to episode of this show.
But to quickly recap who they are, NSO group makes spy work called Pegasus and then sells it to governments around the world, who then, well, spy on people.
It infects the phone and then gives the government full visibility into it.
So when NSO saw how nifty this Circles company was, they purchased the company from Tal for $140 million.
Now, what would you do if you just sold your company for $140 million?
Well, I'd moved to a nice warm island somewhere.
And that's just what Tal did too.
He moved to Cyprus, which is an island nation just off the coast of Israel in the Mediterranean Sea.
But while there, he started talking with another Israeli named Abraham Avni.
Abraham was a businessman and started a company called Pegasus Flight Center in Cyprus.
I think they did charter planes.
And together, Tal and Abraham started a new project, a surveillance tool.
He had an outfit there called, I think, We Spear, We Spear, We Spear, something like that.
It might also be a weird spelling for whisper.
Anyway, Tal started advertising this mobile surveillance technology.
And that's when Forbes is like, Hey, that looks interesting.
Do you mind showing us on camera what you're working on?
And he's like, Sure, come on out.
So Forbes goes to Cyprus and interviews him.
Actually, maybe you don't like to know it, but somebody knows exactly where you are all the time.
Because each of our devices just says, Hey, I'm here every, I think, 15 minutes.
Maybe I don't keep it.
Maybe I don't share it with others, but the knowledge is there.
This video is wild.
It's one of those that when you watch it, your jaw just drops and you're like, What the hell is this?

Tal takes them to his van and then opens the back doors up and there's like two racks of computers, routers, switches, servers.
Inside it looks like your classic FBI spy van.
There's like a desk and monitors and chairs and electronics panels and tenets.
It's nuts.
And Tal is saying, Yes, so this is a nine million dollar spy van.
And here, let me demonstrate.
We send two people out of the van.
We will trace them, we will intercept them, we will infect them.
He proceeds to use Weespear to lock onto these two people walking by and somehow it grabs their data and he's now in their phones spying on them.
It's a crazy piece of technology, but it's even crazier that he was willing to show all this off on camera to be published in Forbes.
I think that's his that's his rep, you know, he's he's known as a guy who like people call him a maverick.
They say that he doesn't play by the rules that he he does unexpected things.
And and I think that I think you could class that video in the category of unexpected things.
Sure. I mean, I think it caused quite a stir when it came out the first, you know, in the first place, amongst people who follow this kind of stuff.
Like it was, you know, it was like, kind of, oh, wow.
You know, this this crazy video has appeared of, you know, we never normally see this stuff.
And it obviously had a lot of ramifications for his business, which perhaps was unintended.
I imagine it was unintended.
OK, so Forbes publishes this video in September 2019.
It rippled through the world, of course, but it also landed on the screens of the people within the Cyprus government.
And they watched it in disbelief, a combination of both the police and the intelligence agency of Cyprus was shocked by this.
They were like, you're advertising more sophisticated spy tech than we have in our own government.
But I think the main thing that Cyprus government got mad about is the fact that he was advertising this business that was being conducted out of Cyprus.
I mean, this whole business is questionable.
Espionage is illegal, you know, and here he's selling tools to do it.
So who knows who?
There are a lot of ethics at play here.
So a few months after this video aired, the Cyprus police decided to just take it down, take it all down.
They move in, they search his premises, they make they arrest some employees, they go through his stuff, they impound the van computer hardware, whatever.
He's out of the country at the time.
They put out an arrest warrant for him and arrest warrant for his business partner, Avni, Tal Dillion, who was absent at the time, he returned voluntarily to Cyprus from wherever he'd been.
That was March 2020.
He got arrested.

He was questioned, he was released.
It's not clear what crimes Tal Dillion committed, but the Cyprus government made it clear that they just don't want him running this business in their country.
And Tal got the message and agreed to pack it up.
He had to move this whole operation somewhere new and looked across the Mediterranean Sea and saw Greece.
Dillion's partner or wife, I believe, is a specialist in creating complex corporate structures.
That's the thing that she does.
Tal began working on the paperwork to reestablish his company in Greece.
And the whole time he seemed to be a bit sore at the Cyprus government for ruining his plans.
Well, he wrote like an angry op-ed, which was published in a newspaper where he basically said that the government was, you know, creating an unfriendly climate for business and that he was going to take his business elsewhere.
And, you know, at least in terms of premises, that is, well, he did do that.
Like he did take his office elsewhere, he took it to Athens.
And this, I think, put pressure on the Cyprus government to change their position.
Ultimately, like, of course, the whole thing was maybe a bit of a storm in a teacup, like, you know, you know, after a year, you know, he was pretty much exonerated.
The police who had carried out the raids were, I think, I mean, it was decided that basically they'd exceeded their powers in such and such a way or whatever.
The whole thing was kind of smoothed over and, I think, eventually could have gone back to business as normal, except by that time he'd already decided that he wanted to set up a new office in Greece.
Now, you might be wondering, is this spyware, malware, virus thing legal?
It's just code.
It's just an app.
To answer that, let's go to Sudan.
In 2003, the Sudanese government had an armed militia called the Janjawid, and they started conducting genocide on the people of Sudan.
It's believed that over a million children have been killed or tortured or raped or injured or just lost a parent in the last 20 years from this group.
And they've been accused of committing crimes against humanity so many times the killings settled down for a while.
But recently, there's been another flare-up.
Silver War has broke out in Sudan.
The Janjawid were back, but they changed their name now, and now they're called the Rapid Support Forces, and the boss of them is Hermeti.
And Hermeti is one of the richest people in Sudan and seems to be funding the war against the people of Sudan.
Now, Crofton, the reporter we've been talking to in this episode, his specialty is tracking airplanes, and he was particularly zoomed in on the
planes that Tau was getting on.
I was trying to figure out if his flights had some connections with the business and his customers.
You know, this plane that we linked to Tau Dili and flying into Khartoum and delivering some surveillance tech that wasn't for the regular army, it was for Hermeti.

And there was a bus stop.
There was like a flare up between the two sides.
And the Rapid Support Forces guys spirited this stuff away, took it out of Khartoum, took it off to Darfur.
This was in, like, May last year.
So when we wrote the piece, there were analysts who we spoke to, you know, spoke about the kind of potentially lethal implications of someone like Hermeti having access to, you know, top of the range phone hacking technology.
So I mean, yeah, to circle back to your question, Sudan's Rapid Support Forces is extremely high on the list of people who it's hard to find a legitimate reason for selling phone hacking equipment to, I believe.
So if Tau is selling his spyware to people in Sudan who are using it to kill innocent civilians, then how much of that responsibility should fall back on to Tau?
The kit he has for sale can be weaponized against innocent people.
Militia groups who are actively killing their citizens, attempting genocide and are accused of crimes against humanity now have this spyware in their hands and can use it.
I think conducting weapons deals with Sudan's militia groups should be legal.
But is this spyware a weapon?
So anyway, that was one of the trade deals that Krofton was tracking by watching Tau's flights in and out of Sudan.
So he heads to Greece and Greece has a new government at this point and the new government comes in in 2019.
Now, I racked my brain trying to understand why Greece, why not just establish a base in Israel, his home country, where he's a military veteran there, he knows people there, he can just operate out of there, but I have a theory, I believe Tau really likes what the NSO group is doing, which is creating mobile spyware and selling it to governments around the world, but he also saw all the heat and scrutiny that NSO group was under.
They have to work closely with the Israeli government to share with them who they're doing business with.
And there may be some restrictions that have been put on the NSO group, like who they can and can't do business with.
And if there weren't restrictions, there is a lot of public outcry and scrutiny of the NSO group of what they should be doing and not doing, which can spoil deals.
I believe Tau saw this huge fire that the NSO group had started and decided to take the wheel and drive right into it, but he would sort of sidestep all the bureaucracy that NSO was tied up in.
If the Israeli government required some kind of oversight into the affairs of NSO group, then forget that, let's set up shop in a different country.
And if NSO couldn't sell to certain regimes, Tau might have saw that as an opportunity to do business with forbidden customers.
Tau knows that some people he sells his spyware to misuse it, but his response to this, well, he told Forbes.
We are not the policemen of the world and we are not the judges of the world.
Which makes me think he may be interested in doing business with anyone.
And if that's the case, I'm not sure he only does business with governments.

He might be selling his spyware to anyone who can afford it.
In 2019, Tau started thinking bigger.
That van kitted out with that we spear technology, he wanted to crank that thing up even higher.
Now, he's not the kind of guy that's tapping away on the keyboard writing malware.
No, what he's looking for are other companies that are already doing that because he'd want to purchase those companies.
Two companies caught his eye, Citrox and Nexa.
Citrox made this phone hacking software called Predator.
And I believe it was Citizen Lab that first showed us a glimpse into what Predator is.
So I'm Bill Marzak.
I am a senior researcher at the Citizen Lab at the University of Toronto.
And I do a lot of the technical work at Citizen Lab in tracking what we call the mercenary spyware industry.
So companies like NSO or Citrox, which makes Predator.
A couple of people in Egypt felt like something weird was going on on their phone.
One was a journalist, one was a politician, and they heard about Citizen Lab
and they've reached out asking them to examine their phones.
That's right. Yeah, we first discovered samples of Predator back in November, December 2021.
It's funny, we were actually checking people's phones for Pegasus, but we found one phone and something else caught our eye,
which was there was a suspicious process running on the phone right when the forensic data was gathered called payload two,
which which struck us as quite suspicious.
Payload two didn't match any previously known malware that they had been tracking on phones.
So of course, it was time to crack this open and look closer.
Right, we could see precisely what input or arguments were passed into this process when it was started up.
And those arguments included a URL, which was was very long, looked looked quite dodgy.
And when we went out and fetched this URL, we were actually able to obtain a binary file for an iPhone, in other words, an application.
And analysis of this application quite clearly established that it was spyware.
It had the capability to, for instance, exfiltrate files from the phone, take passwords, turn on the microphone and listen in to what was going on.
So we were actually able to analyze the the final final payload of of the spyware and understand what it was doing.
And through analysis of the payload, as well as analysis of that URL and the website and the URL, we were able to make an attribution back to Predator.
This was a big finding and they published this for everyone to see.
The report was loaded with tons of information, too.
I mean, not only was it like, here's the malware we found, but it's like, here's what it does.
Here's how you can detect if it's on your phone.
But it also showed the links to how they know that this is the Predator spyware made by Citrox.
But it doesn't stop there.
It goes on to say who Citrox was, who Tal Dillion was, and all these other companies that may also

be involved with this.
And then it goes on to say who those companies may be selling this to, actually listing some of the governments that may have bought this.
Yeah.
I mean, one of the interesting things that struck us about this company or this sort of cluster of companies like Intellexa and Citrox that are behind Predator is there was this very tangled corporate web spanning multiple different countries.
And it was tough to figure out exactly what was going on.
Like, where were the people actually writing the spyware code physically located?
I mean, we did see some references in the spyware's code.
Like they were trying to avoid targeting phone numbers in Israel, even though the company was ostensibly Citrox based in Northern Macedonia.
So there's all these weird links which are kind of a little bit hard to make sense of.
And I just want to stop and show respect for this skill for a moment.
It's one thing to be able to analyze binary files for an iPhone, but it's a whole other skill set to try to determine the geopolitical ramifications for such an exploit being sold on the mercenary marketplace.
You know, in fact, it wasn't just Citizen Lab who was investigating this.
They shared their findings with the security team at Metta Facebook, who was also investigating.
And the combined forces of Citizen Lab and Metta meant that these reports they published were very impressive.
OK, so let's try to connect some of the dots ourselves of what happened here.
An Egyptian politician who was living in exile and an Egyptian journalist were both found to have Predator on their phones.
If two people from Egypt are infected with this, it may mean the Egyptian government is using this technology to spy on their civil society.
Which is spooky. You'd think they'd be using this to stop terrorists or catch criminals, but they're using it to see what stories a journalist is working on next.
This is awful.
But when we back up a second and say, OK, so who makes Predator, this company called Citrox shows up and we see that Citrox was bought by Tal Dillion.
But we also read about this other company called Nexa.
Nexa was formerly known as Amesis.
Amesis was indicted for illegally selling weapons to Libya.
In fact, Amesis was charged with crimes against humanity for helping Libya conduct torture.
But guess what?
While the executives of that company were facing these indictments, Tal started making deals with them.
I don't know exactly what, but at the very least he was using their technology somehow,
either through a partnership or a deal he made with them.
And with that technology, he combined the names together, Citrox and Nexa to form a new company called Intellexa.
Combining this new technology with that spy van we spare stuff he already had,
it meant that Intellexa had quite the arsenal of ways to gather data off a phone and track its location.

And he doesn't seem to be bothered by making deals with a company that's been accused of conducting crimes against humanity.
The report that Meta came up with showed that Predator may have been sold to the following governments.
Egypt, Armenia, Saudi Arabia, Colombia, Vietnam, Philippines, Germany and Greece.
Of course Greece, right?
I mean, Tal was re-establishing his whole business in Greece at the same time.
If he had some kind of partnership with high ups in the Greek government,
then that might be a good reason to move there.
I mean, if he had some connections, then that might help him be able to conduct business without having that long arm of law messing things up.
Well, some Greek journalists saw this report by Meta and Citizen Lab and they're like,
what, spyware may have been sold to the Greek government?
We better write a story on this.
A news outlet called Inside Story wrote a piece basically saying,
look out, Predator may be in the wild here in Greece.
A nice warning, right?
And one person who read that report is a journalist called Thanesis Koukakis.
And he read the report and it made him a bit suspicious
because one of the people who was mentioned in passing was a man called Felix Bitsios.
And Felix Bitsios was someone who Koukakis, the journalist, had been investigating a couple of years before.
And I think seeing the target of his former investigation
tied into the corporate structure of a spy company that was operating in Greece
kind of set off some red flags for him.
And I believe that's what led him to go to the guys at Citizen Lab
and ask him to check his phone.
Right.
Yeah, we started getting some outreach from Greece.
And a spoiler alert, we found spyware.
So the first confirmation we were able to produce
centered around this financial journalist, Thanesis Koukakis,
based in Greece, who had contacted us.
And he was already a little bit suspicious for a number of reasons about potential surveillance.
He noticed his phone acting a little bit weird.
He had flagged some text messages that he thought were a little bit odd.
So we instructed him on how to forward some forensic information from his phone.
We reviewed it.
And lo and behold, we were able to determine that his phone had been hacked successfully with with Predator
in, I believe, it was July 2021.
The Greek paper Inside Story exposed it.
And once news broke out, it erupted in an explosion of articles.
Then the Committee to Protect Journalists chimed in, Amnesty International echoed the story.

The Council of Europe spoke up.
It was news that could not be silenced.
OK, it was kind of a rolling thing that just got bigger and bigger.
There was all kinds of questions and rumors about who was behind the use of the Predator software in Greece
and how it connected to the, if you like, kind of quote unquote, like official phone tapping software.
And this was puzzling, you know, why, you know, is it is it two different entities doing it?
Is it, you know, one entity doing it, but just doing it two different ways?
Like, what's going on there?
And that was that was definitely a question that was in the Greek context that was troubling a lot of people.
Yeah, I mean, one of the really nice things to see in Greece was that there was this such tenacity on behalf of the investigative journalist community there.
They were so invested, so interested in this story.
And we don't really see that in a lot of other countries that that, you know, where we uncover spyware abuses,
perhaps because they're they're more repressive or that there's not as much of a tradition or it's not really in great.
Like in Greece, you have you have this, you know, oh, the birthplace of democracy ingrained in the public consciousness.
So there's there's a lot of people, I think, who feel some responsibility to to take action to to live up to that to that legacy.
So just incredible, incredible work by the by the investigative journalists in Greece,
taking the story forward, constantly pushing the government and ministers for information and driving this case forward.
The Greek government spoke up and said, we've never heard of this predator spyware.
So clearly it's not us.
OK, but now that this story made such a stink, other people started wondering if their phones were being targeted, too.
And so some more Greek people who thought something weird was going on on their phone sent the data to Citizen Lab for analysis.
And yeah, more instances of predator were found.
At this point, three people from Greece's civil society were confirmed to have predator on their phone.
One of these people was a journalist and the other was the opposition leader, Nikos Androlakis, a politician.
Now, by this time, Citizen Lab was getting pretty good at understanding how all this worked.
First, the victim would receive a phishing text message.
And these were crafty phishing messages.
Some of the common themes are really anything that creates or engenders a sense of urgency to interact with the message to ensure that the target clicks on these in a timely fashion.
So, for instance, things about a large unpaid phone bill or something like, oh, you owe the phone company $8,000, you know, it's due in two days, click here to pay or something.
Or, you know, things that are interesting to the target given the upcoming events in the target's life,

like, oh, you have a package delivery is one we see a lot.
Click here to, you know, customize the delivery of the package.
If you couldn't reach you, click here to reschedule delivery or, you know, things like the upcoming vaccine appointment or upcoming, here's your boarding pass for your upcoming flight or here's your registration for this conference so they can use hues from the from the target's life to make these seem very plausible for the target to click on.
Once the user clicks the link, it triggers a series of exploits on the phone.
It may seem like it's just one click, but there's a whole bunch of steps that have to happen for the phone to get infected.
The website exploits something within the Safari browser, which then gets a foothold on the phone.
And from there, it downloads additional malware to infect the phone.
And after a few steps, it then has the spyware binary file on the phone, which is able to watch what's going on with the camera, listen on the microphone, scrape passwords, read texts, and of course, report where the person is.
Now, the tricky thing about this malware was as soon as it would infect the phone, it would erase the tracks of the whole infection process.
So while it may have taken a few exploits to get it to work, those exploits were not visible to CitizenLab since traces of how it got in were wiped.
And this stinks because it means they can't go to Apple and show them this vulnerability that needs to be patched.
It's like they caught the spy and the building would have no idea how he got in.
So you don't know which door or window to go check on.
And you have to think, hold on, if the Greek government paid all this money for this software, surely they didn't get it just to infect these three people.
So who else is being targeted with this?
People demanded that the Greek government say something now that three people had their phones infected.
And they said, oh, OK, um, yeah, well, we've heard of this predator spyware, but that's not something we have.
Flat out denying it for a second time, but people didn't accept that as a good answer.
In fact, they sort of narrowed down who would do such a thing.
And they landed on this must be the work of EYP, which is Greek's intelligence agency pronounced APE.
Because here's the thing, this technology is supposedly only sold to intelligence agencies.
So either they did it or they know who did it or should be investigating to find out who did it.
And if they don't know who did it, then they're bad at their jobs, you know.
So APE has to know something about this.
And this circles back to the Greek Prime Minister, too, because as soon as he took office in 2019, he moved to the Greek intelligence agency to be under the direct control of the Prime Minister's office.
But not all news outlets were angry about this in Greece.
In fact, a lot of mainstream media in Greece was on the government side,
trying to slander the journalists for bringing up these stories,
even slandering the people who were infected by the spyware since they were critical of the

government.
It was a mess.
Now, while all this was going on in Greece, a big conference was kicking off in Prague called ISS World.
ISS World is, you know, it's one of the kind of premier, maybe the premier surveillance technology conference
that it happens a few times a year in different locations.
There's one in Prague.
It's showcasing everything from a large booth featuring hidden away in a kind of inner sanctum presentations of like NSO groups, Pegasus phone hacking tech,
all the way down to like, you know, open source, analytics suites.
I guess, you know, hidden, there's hidden camera stuff there, you know, audio gathering stuff.
But, you know, it's like the mecca of the highest end surveillance technology sales.
You'll find exhibiting there, you know, the world's most famous spyware companies,
like Intellex, like Kandiru, like an NSO group.
Rayzone, Septia, I mean, they're not quite as famous as the others.
But so when you list a bunch of companies like that, I just feel like,
oh, my gosh, there's got to be a huge story for every one of those companies.
Who have they've done business with?
Who have they spied on?
What shady deals are they dealing with?
We keep picking on NSO, but I really feel like just walk into the ISS World Conference
and every one of these companies are any of them above board or any of them like, oh, no, we're, we're very clean or are they all, oh, yeah, this is a cyber weapon that you can use to spy
on your citizens with if you want.
We don't care.
We'll look the other way.
Well, you know, they'll all like, they'll all tell you that they're above board and very clean.
You know, that's a constant refrain of the industry.
And, you know, it goes back to what we said earlier about like, who do you sell to and what are they using it for?
And indeed, to the question of like, do these guys even know, you know, do these companies even know?
Can they know?
A lot of them will say that they they're very careful about who they sell to.
But oh, well, we can't actually monitor what they do with it.
Oh, yeah, that's a whole other degree of responsibility, right?
Because how exactly do these targeting systems work?
Like we have this predator and intellects thing, right?
Like does this whole kit and infrastructure and everything gets sold to the customer?
And then once it's delivered, intellects just kind of steps back and wipes their hands clean of the whole thing.
Or is it some kind of hacking as a service type of thing where the customer tells in Alexa,
here's what we want you to target.

And then intellects, it does all the infections and delivers the data that they got off the phone.
Or maybe it's a mix of intellect said doing the infection.
And once the spyware is on the phone, then the customer can access that data whenever they want,
like listen to the phone calls or see where the person is.
We don't know exactly how involved anyone is in all this.
And you see how this changes like where the responsibility lands, right?
Like, isn't this an important thing to know?
Is the government doing the hacking themselves?
Or is this company doing it with authorization from a government?
I mean, think about it like this, the phishing message that that journalists got,
it looked like a normal article from a financial news website,
but the domain was changed from dot gr to dot online.
And that is what hosted the malware.
So someone had to register this domain, get it hosted somewhere, stage the malware on it
and then integrate it into the predator package and not to mention craft a message
that the target is likely to click on and these domains get burned fairly often.
So you need to create new ones all the time and integrate that into the package.
Is the customer doing all that work or is intellects a setting all this stuff up
to make it easier for the customer to simply point and shoot?
So at the conference, do we get kind of any information about predator?
How much cost or anything?
There was a document that leaked online right after that conference.
Let's see what it was.
This was a predator package for 10 targets at once,
100 successful infections, but 10 running at the same time,
one click infection, eight million dollars.
That was the price tag.
One click infection.
I imagine this means that someone has to click once for their phone to be infected,
which is pretty sophisticated, I'll say, but the brass ring for spyware is zero click
where maybe you could do something like send a message to someone while they're sleeping.
And when the phone tries to process it, like display the preview for what the website's
going to look like, then that preview somehow contains the malware that can infect the phone.
Then when the phone gets infected, the text message can be deleted and you have no idea
that anything happened to your phone.
And so has this capability.
It sounds like it's Alexa wishes they did too.
We're going to do a quick commercial break here, but come back because things
are really heating up in Greece and you're not going to want to miss this.
This episode is brought to you by for Ronas.
So many security incidents are caused by attackers finding and exploiting excessive
permissions. All it takes is one exposed folder, bucket or API to cause a data breach crisis.
The average organization has tens of millions of unique permissions and sharing links.
Even if you could visualize your cloud data exposure, it would take an army of admins

years to write size privileges with how quickly data is created and shared.
It's like painting the Golden Gate Bridge.
That's why Varonis built least privilege automation.
Varonis continuously eliminates data exposure while you sleep by making intelligent decisions about who needs access to data and who doesn't.
Because Varonis knows who can and who does access data.
Their automation safely remediates risky permissions and links, making your data more secure by the minute.
Even when you're not logged in, Varonis is classifying more data, revoking permissions, enforcing policies and triggering alerts to their IR team to review on your behalf. To see how Varonis can reduce risk while removing work from your plate, head on over to Varonis.com slash darknet and start your free trial today.
That's Varonis spelled V a r o n i s dot com slash darknet.
Now, while all this is going on, Croft and Black, the journalist with Lighthouse Reports, was following where Tau's little Cessna airplane was flying off to, trying to make sense of why Tau would be visiting some of these locations.
The Cessna was kind of key to our reporting because, you know, we found out about the Cessna through researching, you know, the company and the people in the company and what they were doing and where they were going.
And that led us to the Cessna and the Cessna obviously led us to a bunch of destinations, you know, not only going backwards and forwards between Greece and Cyprus, going to Prague for the, for the spywarefare, but it was also in Sudan.
It was in Sudan at the time that our sources on the ground said that, you know, this transfer of surveillance tech took place.
It was also in Saudi Arabia.
In Saudi Arabia, it was also in UAE.
We were able to follow it.
We were able to trace it for, you know, a fair few months going around the place.
It was in Israel quite a lot.
So, you know, obviously it raises questions about the extent to which, you know, Tau Dillion is or isn't doing business in Israel because that plane was for sure there a fair amount.
Yeah, but you just mentioned Saudi Arabia and Saudi Arabia and Israel, they're not the best of friends, although you say that, right?
They've got some disagreements.
And I, I just wonder like how much Tau had to say, like, okay, is this million dollar deal worth more than my allyship to my homeland?
Like if people in my country are getting spied on because of this, or maybe he made a deal of like, you can only spy on your own people, Saudi Arabia.
Don't spy on us.
If I hear you spy on Israelis, I'm going to pull the plug on this software.
Yeah.
I mean, I think there's a lot of back channels between these countries where, you know, there's possibly more kind of intelligence cooperation than you might

think, you know, I think that there's a long history of the UAE buying Israeli surveillance tech.
I don't think it's particularly surprising that Saudi Arabia should be a client.
I think these guys are, they're a good market, right?
Back in Greece with this scandal erupting, a newspaper called Documento was saying that they found 35 more people who were infected with this and started publishing the names of these people.
And then every Sunday after that, they kept publishing even more names of people infected with predator.
This list was growing big.
There was a media tycoon on there, a cabinet minister, senior military officials, friends of the prime minister's wife, a respected newspaper editor, and even a popular comedian.
Then the Greek government was asked again.
And this time they said,
Well, actually, it does sound like what happened was that some people got wiretapped and we do wiretapped sometimes, but it's for national security.
And we don't use predator to do it.
But any wiretapping we do do, that's legal.
Well, the pressure continued to mount and was focused on APE, the intelligence department of the Greek government.
You know, we're back in kind of summer last year where there were actually two resignations from government.
One of them was the head of the intelligence agency.
And the other one was this guy called Demetriatus, who was the nephew.
He's the nephew of the prime minister.
And he's also the kind of head at the time of the, let's say, the prime minister's kind of inner office, if you like, this guy is at the top of it.
Now, even though people resigned, the government didn't admit to doing anything illegal.
They said, what happened might have been legal, but it was also wrong.
Now, once these people resigned, journalists and investigators were looking into who these people were.
And it turned out that one of them was the nephew of the prime minister.
And he actually had some kind of connection with the NSO group.
I think they were trying to discuss the Pegasus software a while back.
He quit.
The intelligence had quit.
And it's interesting that on exactly the same day, the plane that we've been tracking that's been carrying out its business based in Greece, but going all over the place also quits and it goes to Israel.
And once it gets there, it just sits there for months and doesn't move again.
Of course, journalists and investigators continued asking the Greek government questions, which led us to learn something new.

The sale of the tech to Sudan was confirmed by the government after the fighting broke out again in Sudan.
Wait, so the Sudanese government said, yeah, we did buy it?
No, the Greek government confirmed that it had been sold to Sudan.
Wait, how did they know?
Well, they issued the export license.
What?
What?
What?
What is happening here?
Someone at Intellexa applied for an export license to sell their spyware to a group in Sudan who is notorious for committing crimes against humanity.
And the Greek government is like, yep, approved.
Go for it.
Doesn't this put some kind of responsibility now on the Greek government for assisting Sudan and the proliferation of digital weapons?
I'm just so tired of things being blatantly wrong in the world and nothing being done about it.
I need some help here.
Hello, hello.
Let me just turn all the vibrations off.
All right.
How are you?
This is John Scott Railton.
He's been on the show a few times and I just like to call him JSR.
He works with Bill at Citizen Lab and he got his hands on this predator malware and analyzed it further.
I told him how mad and upset and frustrated I was about all this.
And JSR being JSR tried to help.
You know, you know, the thing I did first was neuroscience.
That was my old thing.
No way.
Yeah.
Oh my God.
And one of the big things, I was working on neuroplasticity.
And one of the big things that is known about the brain is that anxiety suppresses plasticity and the suppression of plasticity is a good candidate for one of the major causes of depression.
Whoa, whoa, whoa, I'm not ready to get that deep about my feelings right now.
Hold on.
Um, let's reset.
Why I call JSR was because I wanted to talk with him about the ethics of all this.
Not how I get depressed about it.
Okay.

So let's try to understand the implications of all this.
So this world of, I mean, what do you even classify this type of, of software?
Do you, do you call it a cyber weapon?
I like to call it mercenary spyware, although, uh, I've noticed that, uh, a lot of other groups call it commercial spyware, but I like the, the mercenary term in part because it sort of denotes the idea that these people are probably working for states, whereas commercial, uh, to my ear could refer to a much broader, uh, category of things.
Yeah.
And you know, looking at this, I stumbled upon this thing called the ISS world conference, which seems to be just a venue of all these mercenary spyware groups.
That's right.
And I like to frame it sort of like this after Snowden, a lot of governments who didn't really know all the cool toys that the U S government had suddenly not only learned, but were like, Hey, I got to get some of that.
And you have this other dynamic, which is kind of like the first generations of people working within like tier one government programs, developing exploitation tools are starting to look for a bigger paycheck.
And, you know, cushy, cushy approach to retirement thus begins this massive like technology and knowledge transfer from some of the most developed cyber powers in the world towards the rest of the world.
That's the proliferation as people, whether it's from American or German or Italian, um, uh, or British countries are like, Hey, we could, we could really make a business out of this stuff.
And then you add to that kind of this dramatic rise in Israel's high tech sector, combined with a really permissive environment towards export law.
And you get yourself a global industry in this technology.
Oh yeah.
I spoke about this in episode 98, which is called zero day brokers.
There are people who came through the NSA and were developing exploits while working there, and they realized that they could start their own company developing exploits and then sell that to the NSA and make more money doing that than if they were to work at the NSA.
And yeah, some of this tech looks hot.
So I can imagine some other countries wanting this capability too.
And while their internal forces may not be sophisticated enough to develop it, they may have the cash to buy it.
And who knows where they're buying viruses and malware from, you know, so I'm trying to find that line in my head of when this, when this goes wrong.
Where is that ethical line?
And, you know, I've got spy tools myself, right?
I can walk into the store and buy binoculars and a camera and an audio recording device and, you know, I practice hacking things.
So sometimes I've got little devices that can, you know, screw around.

And, you know, some of that stuff's available commercially at DEF CON and nobody really puts a big stink about that.
Like, oh, this is awful.
You're giving this to the criminals of the world.
It just kind of is out there.
But there's something about this that's different.
And can you, do you have a good sense of when that wind shifts to, ah, this is a stinky wind.
It's a stinky wind.
Yeah.
I think that in a democracy, the people who elect the government should have some degree of understanding of how much power the government has to completely pry into their personal lives and when the government can exercise that power.
And what is so scary about mercenary spyware like Predator or Pegasus is that it offers a security service, a total view into a person's private world in ways that we're never designed to respect, you know, existing law about search warrants or seizures or anything like that.
And can just provide that as a turnkey.
So the intent really is to provide this total view on an individual.
I think it's also the case that there are a lot of autocrats around the world who want this technology because they really want to hold on to power.
And they recognize that making their citizens afraid of having their lives basically dumped out on the digital table silently and remotely without any warning is a core part of how they stay in power.
That fear, that technology of fear is a big part of it.
And the fact that Pegasus doesn't respect national borders is a great way for autocrats to basically claw back power into states that they would otherwise have no ability to act in, right?
It shouldn't be the case that an autocrat in Togo has dissidents in the U.K. afraid, but that can be the case when you acquire this kind of technology because you can experience completely devastating consequences of speaking up against an autocrat or a dictator from around the world.
That kind of stuff is just net dangerous to democracy and to freedom.
It appears to me that sometimes when governments get this kind of capability, the temptation is just too high to use it on their wives, friends, their opposition leader.
Like it's just stuff that shouldn't be targeted.
Do you have any thoughts about like, man, this, you've got to really get permission once you, like once you, if you buy this tool, you've got to really.
You know, have a lot of oversight on how it's used or something.
Like, I don't know.
What's the solution there to keep you from being tempted to use it on your enemies?
Well, on your perceived enemies, right?
So like we know from extradition documents, for example, like Panama's then

president, Ricardo Martinelli, apparently got himself a bunch of Pegasus.
Well, who did he put under monitoring?
People like his business rivals, but also his mistress.
And every morning he would, according to these documents, sit and, you know,
put his headphones on in his office and listen to the conversations, you know,
and read the messages of people who he didn't like.
That image of a president angry and jealous,
prying into the lives of anybody who he felt like it is a scary image to all of us.
And it's scary because that's not like part of the social contract, right?
That's not a power that government should have.
And any of the existing powers that government has in a, you know,
a society like the United States are circumscribed by law, right?
I know my rights, you can say, at a traffic stop.
But with something like Pegasus, if, you know, your local police department
has acquired Pegasus and has used it against you, do you know your rights?
Do you know whether they were within their rights or authorities to use it?
Do you know whether their use of it was properly overseen?
What's happening is that this technology is landing in jurisdictions
that don't yet have any legal protections around how this stuff gets used.
Citizens have nothing to protect them.
And that's really, really scary because you want there to be limits
on the power of the state.
Without those limits, you're existing in a tyrannical or autocratic regime.
I just realized something and I don't have time to really research this further.
So I'm just going to go off the cuff here.
But like Google and Facebook, they know a ton about us, right?
They have access to our emails, text messages, friend circles, contacts,
even our location.
And the police have sometimes asked Google or Facebook for the information
on one of their users.
And if given the right warrant or whatever Google needs,
Google will turn over that data to the cops.
And I don't know, that concept alone kind of prompts me to pull focus in
on these big tech companies and how they can spy on us.
Harder than Predator can and it's built into their terms of service.
But the thing that I just thought about is what happens when some other
country wants data on a Google user, like the Sudanese government,
they might be like, hey, this guy here, he's committed some crimes, right?
Can you tell us everything you know about him, Google?
Does Google have to comply with local law enforcement and be like,
well, this request came from your military.
So yeah, OK, approved.
Here you go.
I guess I want to know how does Google handle data requests from

tyrannical or autocratic regimes?
I see what you're saying.
And companies should fight as hard as they can to prevent
these badly formed or wrong requests for this data.
We'd be in a better universe if that stuff was not collected, but it is.
That said, I think that something like Pegasus or Predator
or Quadrim is actually even more invasive in some ways than what those apps have.
In part because your your phone really is, for most people at this point,
it's just like nexus of your public and private brain.
And what's really scary is the idea that governments could access this
secretly without you ever having to know about it and without a warrant,
without any kind of oversight and without any kind of potential
consequence or accountability if they abuse that power,
if they get in there and they use it to hurt you.
And we've already seen cases where the fruits of hacking are used to hurt and harm people.
So as I see this, there is a constant battle
to try to protect a degree of individual
privacy from big, powerful interests,
whether it is governments or corporations.
And we should be fighting this battle on multiple fronts at once.
But what we shouldn't do is say, well, OK, you know,
one one bad apple is already violating our privacy.
So we shouldn't be angry when another bad apple does it.
It's different.
Also, if you think about it like this, it's different when an entity
that is seeking to monitor your behavior in order to sell you something,
learn something about you, then an entity that can put you in jail
and deny you your freedom based on that information has access to it.
And that's why in many cases, I think it's appropriate for the police
to have a harder time getting access to people's private information
than you or I might if we wanted to buy a bunch of user data
because the consequences are so great.
Hmm, good point.
You know, Jack, like as you're talking about these things,
here's here's kind of like how I think about this.
There are certain questions about citizens
that are probably illegitimate for governments to ask certain questions.
Like, you know, do they really believe in, you know, so and so,
presidents, so and so, right?
Because once governments start having the ability
to get those questions asked and to do so in secret,
they may start there may be a temptation to use that information
to retaliate and to harm people.
And part of why it's critically important to stem the proliferation

of spyware like Pegasus and Predator is not just because it's bad
when dictators are able to hack dissidents and chill dissidents.
But because in democracies, we really also do not want this kind of capability
lurking around out there, tempting governments, local, state and national
to abuse it in ways that will ultimately erode the freedoms that we cherish.
Think about this way, like when you make a choice
to speak out publicly against a government policy that you disagree with
in a democracy, you should have some perception, not just that you are free.
You are free to speak your mind.
You can't be jailed for saying, I disagree with this.
But also that it would be inappropriate for the government
to retaliate against you for doing this, right?
And what what form of retaliation is scarier than the idea
that the government could suddenly choose to basically penetrate
as deep as it can into your private world and look at all your stuff.
What a terrifying thought.
That is the thought that people in East Germany live with every day.
That is the thought that people living in dictatorships live with every day,
the potential that an angry official could just be like,
well, let's see what Jack's worried about at 2 a.m., right?
Let's see what health concerns bother him.
Let's see what things he's like talking about in the evening with his partner.
But I think it comes down to why, because if you're if you're trying to say
like we think he's a terrorist and if we want to know what he's doing at 2 a.m.
that's almost legitimate to open up my phone and see what I'm up to.
But if it's like, no, we just want to see if he's going to talk about us
on his next podcast, then then that's a way to hold on that you can't be doing that.
Yeah. So and this is and this is the question like and there are two parts to it.
The first is would they be doing it with proper authority under law?
Or are they just doing it like in a 24 episode
because, you know, there's a ticking time bomb, right?
And spyware merchants love the idea that they're just like all these
terror plots and bad actors and the only thing you can do is key for
Sutherland it and just like hack them immediately, right?
Forget the law. We need to get the bad guys.
But the thing is we know from recent and older history
that if governments start being able to do that, bad things inevitably follow.
Temptation to abuse it always follows.
Some of the biggest problems that we have today in the United States around
privacy come from the post September 11th period, things like the Patriot Act,
right, hugely invasive stuff.
But then the other question and this is just like equally important is does the
society does the governmental office that's receiving this data have the
mechanisms in place to prevent abuse if the people who happened to be holding

this stuff in their hands are not good people or could be giving into the wrong temptations? Part of why it's important that we have laws and rule of law is that you want a person who's got some of the power of the state in their hands, right, like whether it's a cop or an investigator, a prosecutor, politician or whatever, they have to feel that there will be consequences if they misuse that power and they have to know what the guardrails are around how they can use that power.
The problem, one of the big problems with mercenary spy work is that it's arriving in jurisdictions that don't yet have any laws that say how police should or shouldn't or prosecutors should or shouldn't use this technology.
In a situation like that, the potential for abuse is huge in part because like what's going to be the consequence, right?
People in authority might not even believe there would be any consequence if they abuse the technology.
That's part of why people like me feel that it's so important to slow the proliferation down because the faster this stuff arrives at jurisdictions that don't have any laws around this, the more likely you are to see abuse.
I think, unfortunately, we're stuck with the existence of this technology, but slowing down the rate of proliferation is, I think, the best approach we have to limiting the global harm that it's going to cause.
And it is my firm belief that as more and more governments pay attention, they will recognize that a totally uncontrolled digital mogadishu spyware where everybody is using this stuff all the time is a really bad outcome for most governments and that you will need a degree of protection.
The problem is that willingness to act is like, I think, unfortunately, contention on a lot of governments like feeling the sting first.
I don't think it's an accident that a large number of US government personnel had to get hacked with Pegasus spyware before the US took really decisive action.
Well, the US is taking decisive action against Intellexa now.
Reuters published a story a few weeks ago saying the US Commerce Department has blacklisted both Intellexa and Citrox.
They've been sanctioned.
I think this essentially means it's prohibited in the US to do business with these companies and I don't really know how this impacts them.
Perhaps US banks can't do business with them now or maybe it's harder for them to fly on US airlines.
I'm not exactly sure.
But also if they have investors, this doesn't look good for business.
You know, it could shake investors who want to expand to the US someday.
But yeah, that's not happening now.
Intellexa is part of a dizzying web of companies that are operating in different countries.
The parent company is called Thelestris, which is in Ireland for some reason,

and their holding company has declared that they've made $35 million in sales from just doing business in the Middle East.
But other sources have said that they've made close to $200 million in sales in the last three years.
So it seems like life and business is great for Taldilian and Intellexa.
This will definitely be a company that I'll be keeping an eye on in the future.
But with the noise that they seem to be making, sounds like everyone is going to be watching them too.
A big thank you to Croft & Black from Lighthouse Reports for coming on the show and sharing the story with us.
Also thanks to Bill Marzak and John Scott-Ralton from Citizen Lab for telling us what they know.
If you liked this episode, you'll probably also like the episodes about NSO Group, which are episodes 99 and 100.
But also this isn't Greek's first big hacking scandal.
If you want to hear another crazy story about Greece, check out episode 64 called Athens Shadow Games.
If you like this show, if it brings value to you, consider donating to it through Patreon by directly supporting the show.
It helps keep ads at a minimum and it tells me you are more of it.
So please visit patreon.com slash darknet diaries and consider supporting the show. You'll also get 10 bonus episodes there, as well as an ad-free version of the show. So thank you.
The show is made by me, the hesitant skeleton, Jack Reciter.
Our editor is the bare slayer Tristan Ledger, mixing done by proximity sound who just released a book on how to use Pro Tools.
It's called Pro Tools Post Audio Cookbook, 2023, and he's done audio production on films, music and spoken word and jam packs the book with tons of great tips on how you could be a better audio producer.
I'll have a link in the show notes on where to get the book.
Our theme music is by the mysterious Breakmaster Cylinder.
I don't like ultra wide screen monitors because the loading bar on them is just like so long.
This is Darknet Diaries.