

[Transcript] Darknet Diaries / 134: Deviant

Antwerp is a town in Belgium.

What comes to mind when I say Antwerp?

To me at least it's diamonds.

It's the hub of the world's diamond trade.

Well, I imagine if the town is bustling with diamonds, then it's probably also attracting some criminals wanting to steal those diamonds, right?

In 2019, a robbery occurred that really took things to the next level.

It was actually a bank, and it was situated in the diamond trading district in Antwerp.

Monday morning, bank employees came to work and checked out the vaults, but something was wrong with the vault, and they called the police, who had to force their way into the vault, only to find that the place had been robbed.

How though?

The bank had all the right security measures, cameras watching the bank doors, motion sensors in the bank, and sensors in the vault doors themselves, and everything was secured tight.

How did they get into the vault?

They went through the probably six to eight foot thick concrete wall.

They just boreholed, you can actually see three slightly overlapping, kind of like Mastercard logo interlocking circles, boreholes of about a 12 inch diameter maybe, and they just chewed through it over time, getting through the wall, and they crawled all the way through, did everything they did, and crawled all the way out, just kind of army crawled through these, this sandwich shaped hole.

Wow, drilling through a six foot concrete wall, that must have taken a very long time.

In fact, the criminals spent all weekend down there while the bank was closed, so they could make a lot of noise without getting caught, and it really goes to show that if everything is, because the vault had basically been protected to oblivion on the door, and if anyone messed with that door, tampered with that door, tried to torch cut, whatever that door, that was where the alarm was, that was where all the sensors were, all the investment was in the door, because they said, well, what can you do with walls?

I mean, there's not only so much you can do with walls, but you can believe that at least a few bank vaults in Antwerp started looking at their diamonds, and they said, is concrete the only thing that's protecting us, because we got to at least get some shake sensors in these walls, or put one or two cameras in the vault, because if somebody goes in the concrete and they're in there all weekend, that's a problem.

It reminds me of that Bob Dylan song, you know the one, Lily, Rosemary and the Jack of Hearts.

It's a nine minute long song, and it's an epic narrative ballad.

The story summed up is that Jack had his gang try to drill through the wall into a neighboring bank, while Lily and Rosemary distracted the bank owner, Big Jim, and the whole thing takes place in this cabaret?

Lily and Rosemary got the judge and the bank owner drunk, while the boys made their way through the wall, and they cleaned out the safe and took off with the Jack of Hearts.

These are true stories from the dark side of the internet.

I'm Jack Reiser.

This is Dark Net Diaries.

[Transcript] Darknet Diaries / 134: Deviant

Support for this episode comes from Exonius.

Complexity is increasing in IT and cybersecurity.

Support 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 dark net to learn more and get a demo.

That's spelled A X O N I U S [Exonius.com](https://exonius.com) slash dark net.

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.

OK, so who are you and what do you do?

My name is Deviant Olaf and I am a physical penetration specialist.

I have been involved in lock picking, safe manipulation, physical entry, physical bypass, and teaching about covert entry tactics for, well, well, in excess of 10 years at this point we'll say it that way much longer.

OK, so Deviant is a very well known physical penetration tester and we're going to hear three stories about how he's broken into buildings in this episode and the third one is my favorite.

So stick around for that.

But I want to first quickly catch up about how he even got to this point.

I was a network person.

I was a computer person.

I was like a lot of people in the tech world, mostly making my living on a keyboard.

And I liked locks and lock picking and door bypassing.

I knew about these tactics.

It's a very common hobby, but that's, you know, that's your avocation.

I had clients.

There was a law office in town.

The law office had a CIS admin, small and medium business, one stop shop, single guy

[Transcript] Darknet Diaries / 134: Deviant

in an office.

He ran the show with the IT and he just sort of rage quit one day.

Just, you know, table flip, I'm out of here and slamming his office door and he, and it was a pretty crappy law firm.

So I'm not surprised.

But when he left, the staff kind of looked at each other and I don't know if he's coming back.

Is that, well, are we supposed to like do something if that happens?

Because he's got all the passwords.

He's like, what are we doing here?

And of course, you know, you do need to put a plan into place.

They just didn't have one.

So they called up Deviant to come help recover the network.

And he went down there, but the network room was locked and nobody could find the key to get in.

So they called a locksmith to come try to get the doors open.

Now, because Deviant had a little practice picking locks by that time, he took a look at the door.

And I'm looking at just your standard office, standard, you know, standard regular building.

And I'm looking at the doors and then little badge readers, but nothing serious.

And we get to this windowless door, the end of the hall, you know, CIS admin,

IT room, some network, whatever name badge on the door, but it's just a regular door, little badge reader on the wall.

And I said, this is, so it's not like a data center door.

This is just a regular door.

And they said, yeah, but, you know, none of our badges work on the door.

And we don't, like, we don't, apparently even the head, you know, partner doesn't have a key, his key, we thought it was supposed to work.

We'll have to talk to building management about that.

And I said, okay, well, can I try something for a second?

I mean, I'm looking at your doors and I, you know, pick up the equivalent of a TPS report.

I just kind of ripped the cover off of that.

And I said, well, here, if I kind of, and I just shoved a, you know, I shimmed the door.

I just popped it in, slid, toying the door popped open.

And I was like, well, all right, cool.

Well, cancel the locks, I guess, save you a couple bucks there.

And I just breeze on into the room.

I'm sticking flash drives in and the old Pnordal NT boot tool.

I'm rebooting machines and getting, you know, restoring local admin access.

Okay, resetting passwords.

I mean, what was his name?

Okay, so I see his user, I'm just going to kill his user.

There might be maybe backup accounts he made for maintenance, but I don't see immediately a way that he's getting in.

You're probably fine.

I'll, I'll send you a bill.

We're, we're pretty good, man.

[Transcript] Darknet Diaries / 134: Deviant

And I hand, you know, here's your piece of paper with, so here's your new root passwords.
And the guy, you know, the keys to the kingdom he takes it because, yeah, yeah, sure, root password, sure.
And just kind of puts it in his breast pocket.
What'd you do to that door?
And I was like, oh, yeah.
Your doors are all installed with these electronic strikes. They're actually, it's a super common vulnerability.
You can speak to whoever your integrator was about that.
And, you know, he's, hey, Steve, he brings this guy to come here.
Can you show him what you did to that door?
And I was like, yeah, do you want to show it at your office?
I'll pop your office.
So I'm just popping doors open and it bugged him out.
And they said, oh my God.
And that, that became the story of the day, the office.
Not the cis admin who quit, but this kid who came in and opened all the, all the law partners doors.
This resulted in them calling him back to the office to do a full penetration test.
This law firm did not like that those office doors could be open with just a basic folder by just shimmying it in between the latch and the door.
And they wanted to know what else in this building was not secure.
And this got deviant even more into bypassing doors and picking locks.
And breaking into rooms, deviant was good friends with dark tangent, who's the organizer of the hacker conferences, Defcon and black hat.
And dark tangent told him, this lock picking thing, it's really catch and fire.
You should do a training at black hat.
I want you to propose a black hat training about lock picking.
And I was like, no one's going to pay money for that.
He said, no, trust me, trust me.
You know, I think it'll be hot.
You should do it.
And yeah, so that became my career was a law firm who quit and a dear friend who said, hey, people pay money for this knowledge.
Those two forces together really kicked off the idea of doing physical security consulting.
For me and my main colleague through it, through all this has been Bobbock Javadi.
He and I have more than one company at this point doing training, consulting, advising.
And I get to break into safes on army bases.
It's quite a career all from a few little things that you trip over as opportunities.
The first DevCon I ever went to was DevCon 17 in 2009 at the Riviera.
And that's where I went up into the lock pick village and saw deviant demonstrate how the inner mechanics of a lock worked.

[Transcript] Darknet Diaries / 134: Deviant

And you put a right contention bar in my hand and had me practice how to get a lock open. I was fascinated by what he taught me that day. And that's where I bought my first lock pick set. And the lock pick village has grown since then. I also remember a contest that year, which had people try to escape from jail. The premise is that you woke up in a jail, but you had your lock picks with you. So you have to first undo your handcuffs and then pick open the cell door and then pick pocket the guard and then get the lock open to the jailhouse. It was hilarious. And there are a million ways to get a locked door open. You don't always need to pick it in that law firm. It seemed that the latches in the door were installed incorrectly. And by putting a piece of plastic between the door and the frame, you could shim it open. I've also seen whole doors installed backwards where the hinges are on the outside. So you could come in with a hammer and nail and just pop the hinges off and take the whole door off without having to touch the lock at all. And so throughout the years, Deviant has been getting better and better at understanding locks and doors and physical security measures. And I consider him one of the masters in this space. In fact, I'm willing to bet that Deviant has actually given more talks at security conferences than anyone else. Someone did the math and I think they said one of the few people who's talked more than I was was the late and wonderful Dan Kaminski. But again, I just would say yes to everything and I would drive or fly just because I love talking about this. So yeah, it's well in excess of three or 400. That was the last time we checked and that was years ago. 300 or 400 talks about physical penetration testing. Yowzers, how in the world am I going to fit all that information into a one hour episode? Hmm. All right, I got a plan. I think I'm going to take a break, play Elden Ring for like 200 hours and then listen to like as many of his videos and then come back later. Okay, that was fun. And through the magic of editing, I'm back and there's some good stuff that he talks about there. My favorite talk of his is this one. So yeah, this is the elevator hacking talk. This is the talk that we were told had to be on Sunday because because reasons because here's the thing. This is a full one hour talk of him and his friend, Howard Payne, going over so many ways that you can take over an elevator, hack an elevator, and make it do stuff that you shouldn't be able to do. But since this was a talk in Las Vegas where there are a lot of elevators, DEF CON was a bit worried about what people would do with this information.

[Transcript] Darknet Diaries / 134: Deviant

So they pushed the talk back to be on the last day and the last talk of the last day when people were flying home.
So it was kind of a hidden talk.
Where most attendees had already gone.
But it's the most watched video of all of DEF CON's videos on YouTube.
And so it's no secret anymore.
And I think you should watch this video too on elevator hacking.
It'll make you think differently about elevators after you see it.
Like for instance, you may have been in an elevator where you couldn't get to certain floors unless you scan a key card.
Deviants can bypass that.
He can get on an elevator and then get it to go to whatever floor he wants.
He shows you that there are some common keys that a lot of elevators use and they aren't hard to get.
So elevators aren't as secure as you think.
You should probably consider them to be like doors where you really should test the security of them.
And not like an elevator, which is just some mysterious box that goes up and down that only the elevator technician knows how to control.
It's one of those things that I just never thought about.
That's something you need to secure in your building or office.
And that's what's fun about Deviant is how he has all this knowledge of bypassing physical security measures.
And then he loves teaching that to others.
I just imagine you at this point having, I don't know, some sort of matrix style view into locks and security mechanisms that you see.
Like when you pop into an elevator, you just immediately start looking at what kind of keys in this elevator.
How can I turn it on off?
Any door that you look at, is that true?
Or you just kind of like zoomed in on any lock?
It's absolutely, it sounds silly, but it's absolutely, I love that you said it, not me, but it's true.
There's even a talk I made about this phenomenon called Eyes of a Thief.
And corporate audiences kind of like that one, because you walk them through just galleries of images and videos.
And I say, well, here's what you see.
Now, here's what I see and I zoom in and I say, here's this exploit, that exploit, bang, bang, bang, bang.
And my wife is very used to the phenomenon of us walking down the city street and she'll be talking, she'll turn and I'm two steps back because I paused to pivot and take one picture of this building or that car or this fixture or this device and that's going in the slides.
There was a strange paradigm shift when it was you who taught me

how to pick a lock for the first time, right?
And I brought it home and I showed my friend and it just so happened
that my friend's mother was a locksmith.
And she's like, you are not allowed to know this.
Like I asked her in the past, like, hey,
can you teach me how to pick a lock?
She's like, nope, I'm not allowed.
I got like a locksmith code.
I can't show you.
Like it's just, sorry.
And so when I came home and I said, here,
let me try opening your front door.
I want to see if I can do it.
And she saw the tools that I had.
She was just flabbergasted by it.
And it gives me this kind of weird thing of like,
this is kind of sacred knowledge.
Why don't locksmiths, why aren't they physical penetration testers?
Like how come that wasn't just an easy,
hey, like you said, on that job you had, we need a locksmith here.
They didn't think, well, let's get a physical penetration tester here.
And a locksmith doesn't consider themselves
a physical penetration tester.
So why is there a gap there?
Why isn't it all blended together?
Do you have any thoughts on that?
Yeah, I think the real thing there that you hit on perfectly
is the guardedness of knowledge in the old world
of the trade of locksmithing.
If you're doing a physical penetration test,
the value isn't in the success of the tester.
It's in the deliverable.
It's in the report, the knowledge that they will give you.
And giving out that knowledge, physical penetration testers,
yes, we are many times locksmiths,
but much like Penn and Teller are magicians,
but part of their whole shtick over the years
has been showing the audience how they did the trick.
And there are some magicians that think that ruins it,
that it takes all the shine and polish off of it
and that the magic is gone.
But I think that showing in the execution,
if it's elegant and well done and impressive,
it doesn't take away, in fact, it enhances the audience's appreciation for,

[Transcript] Darknet Diaries / 134: Deviant

wow, I would not have been like even knowing how it works,
I would take five years to learn how to do that trick properly.
Same thing with us, I can show you how it works,
but it's not really taking money out of my pocket
or opportunity out of my colleague's portfolio.
If people know how my job functions,
they're not all going out immediately trying to do this job.
There is, as you say, that sort of comprehensive knowledge
of being able to walk through a space
and instantly look and recognize every little detail
that comes with years of experience.
So I'm not surprised at your friend's mother.
I'm not even disappointed.
It's for the longest time that was just part
I was deeply ingrained in the trade.
And why aren't locks, even now as knowledge is opening up,
why aren't they getting into penetration testing?
A lot of them, even with their knowledge as locksmiths,
they can't quite do what we do.
And they're frankly making far,
it's a very different business model,
they're making far too much money.
That's really interesting to me.
If you want someone to break into a place for you, call a locksmith.
If you want someone to break into the place
and then show you how they did it,
call a physical penetration tester.
And while that skill set of both roles overlaps in many areas,
it's just two different mindsets, really.
Um, what is your percentage on,
like when you're going on physical assessments,
percentage of getting into a building?
We've never not gotten in.
You're always going to get in.
The question is 100% success in terms of entering the building.
Yes, every building we've ever seen,
we've been able to enter sometimes quickly,
sometimes it takes a while.
The question is, are we detected?
Is there a response?
How competent is that response?
Can we talk our way out of it?
If we, I've interfaced with guards,
and, you know, had a good story,

[Transcript] Darknet Diaries / 134: Deviant

had an excuse for being there.

Okay, thank you for your time.

All right, sorry.

Well, next time have an escort when you're in this area.

I said, okay, guards.

I want to hear these stories about guards catching him from scouring his videos.

I found three stories he has that I think are great.

So let's get into them.

So this first story starts out

where Deviant was hired to break into a building to test its security.

Their objective was to affect network access

either externally from the parking lot,

you know, cantona or nowadays,

you know, we're not poor hackers anymore,

you get a nice Yagi.

But trying to pick up on, you know, the building's Wi-Fi,

they said, did we, does the Wi-Fi leak?

Or you can try to make internal, you know, connections.

But it wasn't the company itself that hired Deviant.

It was another penetration testing company

that got this job.

But what they were good at was hands-on keyboard type of activities.

And what Deviant is good at is physically getting into buildings.

So this other pentest company hired Deviant

to essentially team up with their computer guy

to get him into the building to plant computers

in the network and gain remote access to this building.

So he was going to get in the building with me,

find an unused network port

or compromise a network port in a conference room.

And then basically just, do they have Mac filtering?

Do they not?

Can I get a device to connect to the network?

Can I not?

Let me see if I can get this little Dropbox headless computer and then it would backhaul off-site.

So he didn't have physical access experience.

That was your job to get him in.

And then once you get him in, you're going to keep watch, distract people, stall whatever you need to do

[Transcript] Darknet Diaries / 134: Deviant

to let him do his job.
Yeah, yeah.
This, it sounds like a good, a good crew there.
It's great.
Like two high skill sets together.
Okay.
And it really, it's a mutually beneficial relationship.
It allows us to specialize only in what we're good at.
Because I am again, not a keyboard jockey these days.
And it absolves a lot of headache and liability
from the primary consultant team.
They say, I don't want to touch that elevator.
I'm not qualified.
I'll touch the elevators.
So what do you bring to this engagement?
So I had kind of a little field bag on me
of some bypass tools, some lock picks.
I did have my elevator keys.
I'll have an under door tool.
I'll have door shims, a mini knife, kind of your typical kit.
Deviant checked out the building
just to get a good understanding of what's there.
Just driving around into the parking lot
and sitting with his car
and watching what the building is doing.
Like, okay, there are security guards there.
But they never go outside to patrol anything.
They just sit at the front desk all day.
On top of that, the building was very quiet.
Not many people at all are coming and going.
And this made them think that
they probably put all their security
at one single point of entry.
And they may not have secured the back doors very well.
So after monitoring the place for a while,
it was go time.
Deviant and the other computer guy
go up to the building in the middle of the day.
They wanted to find a way in.
The two of them started looking around the building
for a way in.
They found some side doors,
but they were locked tight.
No clear vulnerability either.

[Transcript] Darknet Diaries / 134: Deviant

Deviant might have been able to bypass those doors, but he wanted to find an easier way in. You know, that demonstrates a simpler technique that lets just anyone walk right in with like maybe no tools at all. So he kept looking around the building, but was having a tough time finding an easy way in. All the doors were locked tight. No windows were opened. No poorly installed door or anything. So he goes back to that side door he saw earlier and he wanted to take another look at it. Maybe there's something there. Now this side door was a double door. Like you first enter one door and then there's a little room, a vestibule. And then there's a second door that you need to get through to get into the building. And when he looks for a way to get in through a locked door, he has a little checklist in his head that he runs through. It's not like he has some magic tool that he just puts in the lock and the door immediately opens like on TV. He first analyzes the door and looks it over. He'll first just tug on the handle and see if it's unlocked. Then he'll look at the hinges. Maybe it was installed backwards. Then he could just unscrew the door. Then he'll look at the gap between the latch and the strike plate. If this is too wide or missing parts or installed wrong, he can use tools to get in there and open the latch from between the door and the door frame. In fact, any gaps at all between the door and the frame can be exploited. This door had no clear vulnerabilities like that. So then he starts looking at the whole thing backwards. Instead of getting into this door, how do people get out? Is there a crash bar that you just push from the inside which unlocks the door and opens it? Well, he looked through the window, but he didn't see that. He didn't see a handle on this door that you could turn or unlock either, which made him realize what kind of lock he's dealing with. It wasn't a mechanically released door. It was electronically locked.

[Transcript] Darknet Diaries / 134: Deviant

And you can also tell if you're yanking on the door and it's very clearly being held shut maybe with the very top, but the bottom of the door is wiggling by a quarter inch, half inch. You're like, all right, that's a mag lock. That's a magnetic lock at the top of this door. I'm pretty sure we electronically can release that mag lock either looking around or you see it. You don't see any push to exit buttons through the windows. No, it's got to be looking through the window some more. It's got to be a sensor somewhere that where is the, where is that rec sensor? Normally it's right above the door. And eventually we had to look through another window from the side. And my buddy, I was with, he's like, oh my God, is that it? Is that it? Way the heck? It's almost like down into the right where the other door. I said, why the other door? Oh my God. Yeah, that's where they put it. Okay, okay. So there's a motion sensor. If deviant can trigger that, it'll unlock the door, but it's a good 10 feet inside the door. So how? It has a request to exit sensor or rec sensor. These are sensors are very common in physical access control environments, which will detect egress events, impending egress events, and they do it through motion sensors. Most of these are infrared, simple passive infrared sensors that they sense a change in temperature. They presume that must be an individual making their egress from the building. Okay, no problem. So how can you exploit this? If you're on the outside of the building, do you, well, do you throw a fire stick under the door like a road flare, make it hot? Well, you don't have to do anything quite like that. What you can do is take a can of compressed air, or if you're very fancy, you go to a scientific supply shop and you get a can of like tech spray or freeze spray. The idea being if you spray into the air, a little cloud of propellant, a little refrigerant cloud, it will boil off in the atmosphere and make a very cold patch of air.

[Transcript] Darknet Diaries / 134: Deviant

You can do this to open doors.

You stick the little straw through the door crack, blast, and all of a sudden you hear a click.

Oh, that's the lock.

Okay, the lock is released.

Open the door.

This was like that, although the position of the sensor was much further down in the vestibule.

It was a double vestibule kind of door.

And I said, oh man, I'm trying to spray the air, spray the air, and we literally killed one can of propellant.

And I said, oh man, we're going to go back to office max or something.

Eventually, I was able to rig up a long skinny straw that I could feed all the way through,

kind of snaking it down this vestibule,

and almost like a wacky waving inflatable arm of flailing tube, man.

Looking way down at the end of the vestibule,

you see this straw spinning its way all through the floor,

and this cloud going everywhere, and the door finally popped open.

And that was on the floor.

You went under the door.

We had to go all the way under to keep it as straight

as I could on the floor, and it wanted to curve around.

But eventually, I got this door to release.

So you hear a click, and then you know the door's unlocked.

Thank goodness too, because we had been,

this was a good 45 minutes of poking and prodding,

going back to the shop.

Okay, okay, so they successfully made it into the building.

Now they need to find an open network jack.

For the other guy to plug his computer into,

to try to hack into the network.

And we find a little conference room thing.

And I said, okay, look at the, oh cool,

Polycom phone system, and there's an RJ45 connector.

I said, do you want to try this jack?

And he looks in his backpack, and he goes, oh no,

I didn't bring the drop box.

A drop box in this case is a little computer

that you can just plug in and leave behind,

and then try to access it from somewhere far away,

like back at the hotel.

But this guy forgot it.

I guess he was configuring it the night before,

[Transcript] Darknet Diaries / 134: Deviant

and just forgot to repack it, and it's back at the hotel.
He said, well go back, you go back, you take the keys,
here you go, take the car, go back to the hotel.
I'm not leaving the building.
We took so long farting around with that door,
I'm going to stay in this building.
I can just let you back in, when you get here.
And he's like, man, I mean the hotel's 10 minutes away,
and I got to get the thing, come back.
I could be gone half an hour.
You're just going to sit in this conference room?
And I said, no, I'll find somewhere to hide.
So what I did is I chose to look around a little bit,
and I was looking for kind of an empty office,
or maybe a janitor's closet.
Those are nice.
If the janitor's not around,
you can break into the janitor's closet,
and just sit in there silently,
because the guards aren't going in the janitor's closet.
The staff aren't going in the janitor's closet.
If a janitor comes along, you got to, you know,
say I just had some anxiety, I work here,
I'd need a place to chill,
or pretend you're doing drugs, I don't know.
And you say, I promise I'm going to rehab.
Don't tell me, don't knock on me, buddy.
But no, I didn't find any good closets or anything.
I found an elevator.
And I said, okay, well, we got an elevator.
It's got no windows in the elevator cab.
No, I didn't see any cameras.
I'm just going to stay here, bro.
And he's like, really?
I said, yeah, I'm going to put the elevator
on independent service,
which is like a local admin mode
that removes it from general dispatch demand
around the building.
So this elevator cab will not answer hall demand
that other people may be registering placing calls.
I said, I'll just stay in the elevator.
There was even a little, like a little locked panel
that I popped open.

[Transcript] Darknet Diaries / 134: Deviant

And I said, there's even a little power plug in here.
I can plug my phone in.
I'm just going to hang out.
I could just scroll Twitter, read posts on the internet.
I said, you go to the hotel,
get what you got to get,
message me when you're on your way back, I'll let you in.
I thought this would be half an hour of me
just getting paid for free.
It turned into hours.
And I was like, I was messaging.
I'm like, hey, man, did you get to the hotel?
Did you go to the wrong hotel?
What is happening?
Are you, did you fall into a bathroom?
Do you have some bowel distress?
And so I'm thinking, what is going,
finally I get an answer where he's like,
yeah, it's not going well.
And I said, what's not going well?
And he's like, I'll tell you what I get there.
He was found a little frustrated.
Hey, I'm getting paid by your company either way.
I'm on the clock.
Back to Twitter.
Two hours go by.
Deviant keeps messaging the guy.
What's going on?
He says he had to finish setting up the Dropbox,
but he couldn't get the keyboard to work, to configure it.
So he was trying to use the on-screen keyboard
and use a mouse to type out every command.
And it was just taking a super long time.
So Deviant continues to just sit and wait.
Then suddenly I hear this really.
Like this pounding noise sounded like it was on the hoistway doors,
just someone banging on the doors of the elevator.
And I went, holy crap.
Did they know I'm in here?
Have they spotted me?
And I'm looking, maybe there is a hidden camera.
What's going on?
And I said, no, calm down, calm down.
It's like if you're camping, everything sounds loud in the woods.

[Transcript] Darknet Diaries / 134: Deviant

A deer could walk through your camp at night
and you think it's a bear.
But I said, no, all right.
It's, I look at my phone.
I'm like, all right, it's, it's like after five at this point.
This has got to be the cleaners.
They must be, I don't know, getting fingerprints off
of the hoistway door chrome or something.
I don't know.
But I just said, no, it's fine.
And I stayed in there a little longer.
I really wanted to start to use the bathroom.
Thank goodness.
My buddy's like, all right, I'm coming back to the hotel.
I'll be there in a minute.
Okay.
Elevator back to automatic.
Go back to the lobby, open the doors.
And I said, I'm right near the vestibule.
I'm going to head toward it.
But just, I don't know what made me turn and look
as the elevator was shutting itself automatically.
I noticed that there was literally a notice
that somebody had taped on the doors.
Because I had been sort of in between two floors.
I've been a little bit off platform, but I could hear,
I was right near the lobby level.
They were in fact hitting that door, but it was a security guard
taping a notice that said, this elevator out of service,
yes, we're aware of it.
We're looking into it.
Please use elevators on North Bank of the building.
And I went, oh man, I guess somebody noticed I was in there.
And just, thank goodness they didn't think I was there.
I let my friend in.
He's in the building now.
Thank goodness we didn't have to fight with the long straw.
All right.
Let's back to the conference room, back to the conference room.
Okay.
And we barely got six or seven steps down the hall,
when around the corner, we see a guard.
Because now we're the only ones, now it is a little weird.
At this point, yeah, what are you doing?

[Transcript] Darknet Diaries / 134: Deviant

It's after five, this place is dead.
And the guards look at him, look at me,
walked in and my friend is like, oh, what's going to happen here?
The guard immediately saw that I had,
because I was in the elevator for so long,
I had put a little badge on that just said, Otis,
you know, I have a variety of little badges in my kit.
And he went, looked at me, look at my Otis badge.
And he went, oh, you guys got here fast.
And I was like, yeah, I heard there was a,
and I, you know, I just, I lie for a living.
I just dropped into it.
My friend, I don't know if he was nervous or not,
but I said, yeah, I heard you had a problem
with one of your passenger elevators today.
They pulled us off of some other job,
because you're paying for this elite care service.
You've got a good tier of service package with us here at Otis.
Point me at the problem, let's get you squared away.
And he proceeds to lead us right back to that elevator
where I had been with the notice still taped on the,
you know, the door.
And he's like, this frigging thing, I got calls all afternoon.
And so now I like this.
I like that this guy, he's invested in the problem.
He's invested in it being solved.
And I said, oh man, that's,
and it's only elevator in the bank.
You don't even have other cabs that you must have been,
your phone must have been ringing nonstop.
He's like, oh, well, there's not a lot of people in here,
but they, they sure let me know about it.
I said, well, let me see what I can do, sir.
I pull out my keys.
I still have my keys.
The keys will turn obviously in all the key switches.
So I, I have the trappings of legitimacy where I,
A, look like I have credentials,
B, I'm sympathizing with his problem.
I can express familiarity with his problem.
And then C, I am pulling casually pulling implements
out of my pockets that clearly work in the system.
If you were in a parking lot
and you saw somebody with a red blazer

[Transcript] Darknet Diaries / 134: Deviant

and they, you thought they might be a valet
and they say, oh, is it really busy
in the restaurant tonight, sir?
And then they are holding a key that opens a car door.
Clearly you might, well, that's gotta be the valet.
They, they're doing all the things
that I've seen valets do.
So this guy just thought, well, he's obviously the Otis guy.
And I'm, I'm rattling off some techno jargon
and I'm turning key switches that don't do much,
but I'm claiming, oh, I'm, I'm resetting the door sensors.
Now this will reboot the door operator
if we hold it for three seconds.
Here, let's everyone step into the cab for a second.
Let's let this door close.
So now I'm bringing, we're bringing the guard with us
and the doors close.
And I say, all right, well, that's good.
Let's try door open.
No, we're still level.
We're not misleveled.
Sometimes a mislevel event can cause the doors to jam.
Let's try to go up a few floors.
So he just starts taking us up to other floors,
floors that I didn't have credential access to,
but he's going up floors
and we're stuck in platforms pretty well.
I'm pretending to measure the platform leveling
because again, I have just enough industry knowledge
to speak to what you're expecting a technician to do.
I'm actually a, you know, I'm a trained
life safety fire door inspector,
not because I do that for a living,
but because I can walk around a building,
if anyone catches me and say, what are you doing in here?
I can say, what are you all doing in here?
Because these fire doors are not to code
and I can rattle off all the different,
the signage is wrong, the glazing is this,
you can't have a pertinences that interfere with that.
So I look like a technician, we're getting up,
we finally get to the top floor,
which is a really juicy floor in this building.
And I say, let's walk around for a minute here.

[Transcript] Darknet Diaries / 134: Deviant

This, I think this one,
you said there's another elevator.
I'm pretty sure this one's fine,
but let's try the South Bank elevator,
the North Bank elevators.
And now the guard is so used to being in our company
that even anyone else who's in the building
who sees us on camera or in person,
well, this guy has been with the guard,
so he must belong here.
And I start spinning a story about,
do you have a room with a bunch of computers in it?
Because your elevator controller would be in that room,
it would not be in that room.
So, but where's the elevator?
I can look for the error log data on the elevator controller.
We can try to troubleshoot it
because you don't want to have us coming out here again and again.
Those stoppages, that was no fun for you.
So yeah, the guard took us to,
he's like, well, I walk around every night,
and this is the one room.
It's got all these fans in here.
So he takes us, and I think my badge works, boom.
He badges us into the server room.
And I say, all right, well, you help me look.
It is going to be a bright neon green server,
so which is, again, I'm making that up,
but I'm giving him a wild goose chase.
But do you turn to your buddy and be like,
this is the moment you need to go now.
He was tracking at that point.
He knew what was up,
and he was amazed that it was working so well.
But he was ready to go.
A good friend will see you lying,
and it's all improv.
It's all yes and.
You just go with it.
You build the world with them that they're trying to build.
So my buddy was ready.
He had the dropbox kind of under his arm,
like it was a multimeter, ready to plug into something.
And the guard goes down one aisle.

[Transcript] Darknet Diaries / 134: Deviant

I go down another aisle.
Do you see it over there?
And my buddy, of course, he's plugging stuff in.
He's plugging in flash drives, watching, documenting.
And the guard eventually says, well, I can't find it.
We can't find it.
I said, all right, that's all right.
It's working for now.
I'm going to write it up.
I'm going to write it up as a priority ticket.
We'll get you squared away.
What was your name again?
And he gave us a name.
I said, okay, well, we're going to walk around,
just check.
There's a few other lifts and other buildings.
If anyone else is on premises and they ask what we're doing,
I'll just tell them to talk to you.
But thanks for all your help.
It's all good.
And he was so happy that, yeah, we stuck around.
Even though we were done, we stuck around
and went into a few other spaces,
just in case we got challenged.
Because you want to give the client a win.
You want to try to see, will anyone push back on you?
It's not about getting away so clean and so,
if you work for the government
and you're spying on a foreign adversary,
sure, you want to get away and not experience a mortuary event.
But if you're doing a corporate test,
you want to see what their reactions are.
If this staff didn't catch you,
interface with a different staff member.
If this building didn't stop you,
try a different building.
Where are the good as well as the bad
in their security posture?
But yeah, we wound up walking everywhere
for quite a long time.
We got into everything at that facility
at the end of the day.
And digitally and mechanically and physically, yeah.
There are three things to test

[Transcript] Darknet Diaries / 134: Deviant

when testing a company's security.
You can test the physical building itself.
You can test the people in the building.
And you can test the electronics.
This one tested all three.
But there's kind of a moral code
that Deviant has when testing people
or otherwise known as social engineering.
I mean, here he tricked a guard
into making him think he worked for the elevator company.
But he also gave the guard many opportunities
to check his credentials or verify who he is.
Gosh, even if just the guard decided
to give him a visitor's pass
and took their names down,
that would be better than nothing, right?
So there were lots of training opportunities
for this guard.
But bad guys don't really have these moral codes.
They might wrestle the guard to the ground.
Tie him up in the elevator
or break some windows to get in.
I mean, it's possible to figure out
where the owner of the company lives
and kidnap their kids,
holding them for ransom for some company data.
But as a social engineer,
you really want people that you trick
to feel better for having met you
instead of feeling awful
because you screwed them over so bad.
But where exactly that line is?
It's hard to say, though.
We're going to take a quick break here,
but don't go away.
We have two more stories from Deviant
when we come back.
This episode is brought to you by Foronis.
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

[Transcript] Darknet Diaries / 134: Deviant

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 Foronis built least-privileged automation.
Foronis continuously eliminates data exposure
while you sleep
by making intelligent decisions
about who needs access to data and who doesn't.
Because Foronis 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,
Foronis is classifying more data,
revoking permissions, enforcing policies,
and triggering alerts to their IR team
to review on your behalf.
To see how Foronis can reduce risk
while removing work from your plate,
head on over to
Foronis.com slash darknet
and start your free trial today.
That's Foronis spelled
V-A-R-O-N-I-S dot com slash darknet.
So a company in Kansas heard about him
and hired him to come out
to test the security of their building.
And it was a small town, man.
It was a small town.
So this was a company doing large sort of,
you know, blue collar industry
in a small town where I'm not from.
And the only thing I got going for me
is that I'm a middle-aged white dude.
And that's where my flex ends.
Because I don't know people in this town.
I can't speak to the widgets and wonkets
that they pack into boxes and parcels
and drive out on a big rig.
I was going in.
We'll see how this goes, boys.

[Transcript] Darknet Diaries / 134: Deviant

Being so far away,
he had to fly out and rent a car
and then drive to this town.
And he didn't go alone, of course.
He had two others with him
who also worked at his penetration testing company.
And one of his teammates brought his dog with him.
She's a search and rescue dog.
She's amazing.
Because a dog is so perfectly trained.
You could let her off the leash
and she knows commands where she could,
you know, run
and just kind of be hidden in the woods.
And so now he's a guy walking around with a leash.
And who doesn't want to help a guy with a dog leash?
Of course, you got that beautiful dog of mine.
So eventually, you know,
he'll come running out if he gets challenged by...
Oh, here's my dog.
Thank goodness.
Holy cow.
The dog is a social engineer too.
It's part of the act.
Go hide while I pretend to look for you
and wait for me to give you the secret command
before you come.
Oh, man.
I never thought of packing a dog
in a physical penetration testing kit.
But they're going to need it
because this place looked really hard to get into.
The goal was to demonstrate access to quote sensitive areas
with a list of sensitive areas,
manufacturing areas,
certain people's offices
that were in charge of critical functions.
If we could demonstrate,
we could tamper with end product
before it goes to market.
That would be bad.
And you know, you just tamper.
It means you touch hands on this one machine
or this one package and take a picture.

[Transcript] Darknet Diaries / 134: Deviant

So why don't you think you can get in?
What's the thing there that you're like?
It was a small crew.
I mean, it was maybe a dozen employees on any shift
and everyone knows each other.
And it's not an environment that was open to the public.
So it's not like customers or visitors
were coming and going,
which is much more common in offices.
You know?
Yeah.
If we were on site,
not to mention we had to read all their briefing materials
on their OSHA regs
and their best,
best industry practices.
So if you're in a production environment,
you've got the hard hat here,
you've got this,
you've got the earplugs.
Otherwise, the foreman will be safe.
Who is that person who lets you in here, jackoff?
So we wanted to minimize contact with humans.
We would go at night, we said.
And we would try small town America.
You play to what you think is going down.
You say, it's either going to be Saturday night football
or Sunday.
Everyone's maybe at church.
I don't know.
So Saturday night,
we started to weaken the target.
So we'd approach.
We would remove card readers from their mounts.
It turns out there was an open campus.
You could walk onto the grounds.
There were no fences.
But we would remove card readers from the wall.
We would install little interception devices
behind the card reader,
put them back on the wall.
It's a device called an ESP key.
Like, all right, we're going to check a few doors.
The doors are all tighter and all tighter,

[Transcript] Darknet Diaries / 134: Deviant

tight as a drum.
We'll compromise the card readers.
Hopefully somebody coming or going on a late shift,
because they did have a very,
they worked in three shifts.
Maybe someone's going to use a door
and we'll be able to compromise the credentials.
When we come by tomorrow.
Sunday, there were no,
there was, we asked,
do you have any hours on Sunday?
They said, nah, it was pretty spin on Sunday.
Okay.
I mean, production environment,
the actual factory was running,
but the offices were dead on Sunday.
They said, okay, come by Sunday morning.
And we drove by the parking lot,
just pulled in and pulled out,
enough that I could dump the remotely.
I could radio into the interception devices.
I got some credentials.
Good.
You caught all that, right?
There are RFID key cards that employees use
to unlock doors to get into the building.
Deviant installed a card sniffer behind the real card reader,
and someone badged in during the night
and his sniffer caught that.
And now he has that data
and can write that onto a blank key card,
which would give him access into this building.
Now, while he was doing that,
another one of his teammates was hiding out,
watching the building from a distance,
taking pictures of people coming and going.
And this guy had a camera
with a long-range zoom lens,
so he was out there taking photos
of what badges looked like for people who work there.
He couldn't get high-quality close-up photos
of the badges being that far away,
but it was enough to allow them to replicate it in Photoshop
so that if someone is walking by or from a distance,

[Transcript] Darknet Diaries / 134: Deviant

they wouldn't know the difference.
So the team all met up at a coffee shop
to put the right logo on the badge
and to write the data onto the key card.
And as we're there, my buddy, the guy who has the dog,
he didn't have the dog at this moment,
but that one partner,
he's like, I'm just going to take one more walk around,
just see the factory.
Let me get myself a little coffee or something.
And he comes back to where we were
as I'm making these badges.
He comes back 20 minutes later.
He's like, this is going to be interesting, man.
I just stuck my head in at the post office.
Everybody knows.
Every, hey, Frankie, Sally, how you doing, Bobby?
And it's like, if we run into anybody,
it's going to be a record scratch.
It's going to be weird, man.
But we said, all right, we've done this.
We've been in hard jobs before.
Let's go, everybody.
We pull into the parking lot.
We had some PPE and hard hats with us,
looking vaguely factory-ish.
So you're looking like employees
that should be there or technicians visiting?
Just looking like employees.
If anybody literally, like if a town cop was going by,
we're like, they'll think we must work here.
We look like blue collar workers.
And sure enough, nobody, no police.
It was right on Main Street.
It was a tiny, tiny town.
But this factory was right in the middle of town.
It was the only thing in the damn town, honestly.
So boop, card reader works.
Okay, we get in one building.
Thank goodness we're inside.
We're walking around.
Once you're inside, a lot of buildings,
security's a little weaker on the inside.
You can get into offices.

[Transcript] Darknet Diaries / 134: Deviant

You can slip a latch.
You can pop a drawer open.
We've found a company.
Trucker cap.
Somebody took a company jacket.
Again, just you're looking a little more like you belong there.
And the thing is, the badges we made,
we had seen long-distance photos of their badges.
So I had pre-printed these badges with their logo and everything
and roughly the right place to look.
The badges look the part and the badges are open indoors.
But within maybe half an hour,
we hear one of my teammates come around.
He's like, hey man, someone just pulled into the parking lot.
Not to the factory.
Somebody pulled in and they're coming into this office building,
which no one is in this office building at this Sunday.
And we're like, oh, well, we just look like we're working here.
We sat kind of in the break room area.
And this guy comes in.
He must have been 56, 57 years old.
He's like, how do you do gentlemen?
Say, hey, how's it going there?
Can I ask what you're doing in the office today?
And the vibe was instantly off.
We said, oh, well, you know, we're just checking.
We had a story.
I think we said we were doing an environmental audit.
We were checking door seals.
He was in the building?
He was already in the building.
How did he get in?
So he clearly worked there.
Okay.
He was clear.
And we could see on his hip, he had a badge.
And we said, no, we're just checking some door seals.
There were some door closure issues.
And for regulatory compliance,
you have to keep products separated, blah, blah, blah.
We had a bit of a story.
And we said, well, you know, we'll get out of your hair.
We're just leaving this building anyway.
Not to, and we kind of left the building.

[Transcript] Darknet Diaries / 134: Deviant

And the guy didn't quite, he didn't quite vibe on that.
He was looking at us a little weird.
Well, this was mostly a success.
They needed to demonstrate access to sensitive equipment and areas that they were able to get into the building and take pictures of them touching this equipment and stuff they just shouldn't be able to get to.
But since this guy really wasn't buying their story, they decided to leave.
Because as a penetration tester, when you get caught, you want to see if you can get out of that situation.
Try to leave and get out of there.
See what happens.
Is this guy going to stop them from leaving?
So they walked out and got to the parking lot.
And they could get in their cars and go, but there was another building in this parking lot that they also needed a test.
So might as well walk over to that and see what happens.
They thought this guy might be watching them though.
So they walked across the parking lot to the other building and made it very clear in case he was watching them that they had badges that they were using to get in the building.
These were working badges.
And if the guy was watching them, he could see they had valid key cards to get in the building.
Don't forget on top of that, they have a jacket and a hat with the company logo on it.
And then we in the new building, we're like peering out the windows through the blinds.
And this guy walks to the parking lot with the guy who's going to get in his car.
Nope, walked by all the cars, walks to the building.
We just got in.
We're like, oh my God.
And we hear him start walking around this building.
And at this point, we're pretty sure we're roasted here.
Two of us break off.
One guy goes, he meets two of the guys in some other hall.
He's like, excuse me, gentlemen.
I'm going to ask the same question I asked before.
What are you doing in this building?
And we said, well, we're doing this.

[Transcript] Darknet Diaries / 134: Deviant

He's like, no, no, who hired you to do this job?
And we said, well, it was, it was, you know, Francis.
Francis in HR, she brought us.
He's like, I don't know if Francis would have brought you on.
I'm going to have to try to call Francis.
And he couldn't reach her.
And he said, and we, and he's dying.
It was like, no, no, come on.
Was Francis a word you made up?
No, we knew, we checked their staff.
We knew some staff.
We said, no, Keith at the, at the, you know, the Wyoming plant.
Keith knows that we're here.
He's like, I've been working with Keith for a long time.
Keith might have said something about new folk.
I haven't heard that.
I can call Keith.
So we're like, oh my God.
And eventually after he's getting,
he keeps trying to dial phone numbers on Sunday.
And we realized if he's not going to reach anybody,
he's going to just call law enforcement.
This was not going to fly.
Deviant and his crew were caught.
All the windows of opportunity to lie their way out of it were closed.
The game was over.
So time to come clean and show the get out of jail free card.
See, here's the thing.
When you're paid by a company to break into their building,
it's possible it could all go wrong.
So you need a letter of authorization from the company,
preferably someone real high up that can vouch for you,
that when you call them, they will say, yes,
we did hire them to do a security test on the building.
And you print this agreement out
and put it on a piece of paper and carry it with you at all times
when you're doing a physical penetration test like this.
And this is what's known as the get out of jail free card.
Now, what some penetration testers do is they print off a fake one.
It's got the right name of the head of security,
but with a phone number to someone waiting in the parking lot
who would act like that person if they got called.
Deviant saw that this guy had everyone's number in his phone already
and thought the fake get out of jail free card isn't going to work here.

[Transcript] Darknet Diaries / 134: Deviant

So he gave him his real one.
And this was the first and only time Deviant has ever been caught to the point that he had to show this paper and come clean like this. He said, I know that person, but I'm going to call her cell phone and not the number that you've printed here.
So as it turns out, and we spoke to him, he said, okay, all right, well, if you say so, all right, Susan, brilliant.
He did not trust the number on the paper that Deviant handed him. Instead, he looked up the names number himself.
And this was the right thing to do.
And sure enough, the head of security vouched for them and said, good job catching them.
And yes, we did hire them and they are supposed to be there.
So now that he knows the real reason Deviant and his crew were there, Deviant had to ask, how did you catch us?
But he's like, well, I was driving by.
He wasn't even on site that day, but I was driving by and I saw a couple of you boys enter in the building, just as we were just getting into a door.
He's like, it didn't feel right.
So I got a block or two down the street and I turned around and came back.
Who in the hell gets past their office and has that much emotional investment to go, I should go back to the office and see if he drove all the way back in, parked and started checking around buildings till he could figure out why were these fellas he didn't recognize from 200 yards away.
Why are you in my building?
He had worked for this company for something like 38 years. And he had just, he had emotional investment in the company. The company mattered to him as a person and he was not going to take anybody giving him a line.
He said, no, I want to know what you're doing.
And it felt like if someone was in your backyard and they said, well, I'm just trimming your trees for your neighbor. But they kept kind of walking through your backyard.
You might be like, I'm going to knock on my neighbor's door. Why is this person in my backyard?
So that's what happened.
And we, that was the first time we ever had to show the action. And we knew we could have had a fake letter but we're like, that's not going to fly.
This guy, he has switched on, he is sharp.

[Transcript] Darknet Diaries / 134: Deviant

And he got quite a little kudos out of that.
And he was professional the whole time.
Didn't try to tackle us, didn't make threats.
Just kind of slowly plotted after us.
Okay. So they were caught.
That's that, right?
No. They said, hey, good job.
You caught us.
But don't tell anyone else
because we're going to go and come back again later
and try to see if anyone else will catch us.
We left for a few hours.
We went to have lunch.
We did come back.
And we only made it in again, gosh, 45 minutes, an hour
until we ran across some other person.
And I didn't even interact with this person.
This was just in a production
if I just kind of walked past them
and they almost on their heels turn and spun and said, hi,
can I help you?
What are you doing in this space?
And we were like, son of a bitch.
But that was a great day because we, you know,
this, this little nowhere'sville facility
they had a really sharp head of security
who had been coming to DEF CON and Black Cat,
watching talks like mine,
really investing in upgrading their locks
and their access control credentials.
And even after that, he's like, oh, you did clone.
You made the ASP key.
We're going to, we're going to revamp our backhaul protocols
for a little nowhere factory, nowhere, nowhere,
not, not subject to threats and not subject to robber.
The most threat they probably have is people trying to break in
and I don't know, steal copper or something, you know,
like rural threats are not the same as an urban environment
where you have a lot more potential risk of different kinds.
But no, this one guy, he was really all about it
and he took it to heart.
He taught, he had a lot of buy-in from management
and everyone was just, they were pleased
and proud of their people.

[Transcript] Darknet Diaries / 134: Deviant

We told them, keep investing in your people.
They like it here.
Make sure they keep liking it here
because they are the best line of defense
that we've ever come across.
You were caught.
Do you consider this a caught?
Do you consider this a failed?
Is this, is this the only time you've ever been caught
or have you been caught before?
I will consider it a caught.
I won't consider it a fail because this is,
if you're doing your job right,
this is the best success you could have.
We got caught for all the right reasons
and I'd like to get caught like that much more in the future
by companies that have employees that actually care
about what's going on.
The only way you get that is if you have a real nice environment
where you're treating people well,
not just as meat grinding through the mill, right?
You actually have to make people want to work there
by rewarding them, by paying them properly,
by giving them real benefits.
That's the only time we've been caught
and didn't bluff our way out of it,
you know, talk our way out of it.
Okay, let's hear one more story of DV
and breaking into buildings.
And this one's my favorite.
This one is against a critical infrastructure type company.
Think a utility company.
If someone were to get in and cause harm,
it could be ruinous for like the whole town.
Most of our jobs, we get a list of sensitive assets
or sensitive areas from the client.
And we say, what, you know, would accessing this asset
or being in this space represent a severe breach?
Would a bad actor in this space
have the ability to severely compromise operations
or cause severe impact?
Once you have that list of assets,
you formulate a series of attack chains.
You sit with your team after a lot of recon

[Transcript] Darknet Diaries / 134: Deviant

and you say, all right, so do we think
it's smart enough to go to this one first
or should we try to go through this one?
We've identified where these assets are,
which parts of the buildings and the grounds.
Okay, so which team is best suited
to position here, here, here?
And you come up with a plan.
And if one team gets burned, you'll say,
okay, well, that team is, all right,
they might have gotten noticed, might have not.
Let's pull them back.
Let's get off campus.
They just became overwatched.
They're running a drone.
They're running long range cameras.
They're back at the base on radios.
Let's put another team in.
We do a lot of rotating out of rental cars,
where you go back to Hertz or National or somebody,
you say, oh, the car's pulling to the left a little bit.
They say, we have another one.
I said, do you have a different model?
Maybe a really different color,
because they've somebody seen that weird car
in the parking lot.
So there was a job like that.
It was meticulous and we had, it was a large job.
There were probably three or four different field teams
at any given time of pairs of people.
Okay, well, this is a big job.
And if you remember from other stories,
Deviant likes to be prepared and bring a big kit of things,
anywhere from having lockpicks and keys
to the Otis elevator repair shirt
and having long range cameras
and full badge printing machines.
But this one, he needed even more.
This job was the kitchen sink, man.
This job had case upon tons of Pelican cases shipped in.
It was close enough that I could,
it was many states away from where I was at the time,
but I was living in Montana.
I just said, I'll drive.

[Transcript] Darknet Diaries / 134: Deviant

If the budget's there for me to drive,
I'll make it a couple of day drive.
And my truck was, I mean, we brought the works, man.
We had a 3D printer in the Airbnb.
We had a couple of our really large key machines,
our exotic key machines,
just in the Airbnb on the living room table.
We were ready for as much as we could be.
Okay, so when you have a job this big,
it'll help if you have a few extra people.
Of course, Deviant drove out for this,
but a half dozen other people came out too.
Bobbock was also there.
We're all across discipline.
Bobbock is very electronic focused.
Of all the team members,
he is the highest strength among us
in the electronics department,
especially as it relates to access control technologies,
credentialing technologies.
He gets good information from a lot of the industry sources
and partners where he'll get the new badge printer
that somebody's just pioneering
and he'll get a sample model of that and we'll try it out.
Drew came along for this one.
Drew is our main surveillance person.
Drew is an incredible person with camera glass,
drones, you know, ultralight aircraft.
He is the eyes on the ground and in the sky.
They called in Sophie too.
Sophie is a devastating social engineer.
Robert was another key player here.
Robert is an incredible physical tactician
along with being personable with people to the drop of a hat.
I mean, he used to be a cop, right?
So he can lie through his teeth with a smile on
and his job is to manipulate you as a human
because he's going to get what he needs
and he's going to get it out of you for information
or he's going to get out of your sights
because he wants to move.
He can be front and center or he can be a ghost.
Imagine being called a physical tactician.
That's quite the title, isn't it?

[Transcript] Darknet Diaries / 134: Deviant

Drew and I reached out to an old colleague of mine named Laz, who was back east.

We brought Laz in.

We had a couple of interns at the company who wanted to get some exposure to field work.

And a lot of times jobs just aren't big enough, but this was great.

So yeah, they bring the interns.

So we had quite the cadre of people and we actually had two Airbnb units right next to each other.

We had so many people.

It was these two little like cabin type houses on some park somewhere.

Gosh, they rounded up the whole Ocean's Eleven crew for this job.

And so they all met at the safe house and started on phase one, surveillance.

That was almost a week of recon.

Yeah, that included driving by for the first few days, just a lot of long range camera work in cars,

which led to then hikes through fields,

where it was a lot of Drew and Robert just in like,

I mean, they're in hunters camo.

They're hunters and stuff, right?

So like they're going to crawl through field.

They were first like walking,

and then they were low crawling

to get really up close to the buildings.

See, I don't quite get this, right?

Some engagements, you're just like,

let's see if we can walk into front door.

Let's go.

And then some engagements, you're like,

okay, you feel like getting muddy.

Oh yeah.

You feel like getting, you know,

this special equipment out.

Like, I mean, there's work to that.

Like, dude, really, you really want me to crawl through the mud so I can get a good photo.

Yeah.

Yeah.

Go under the fence there, do it at night.

And we were all about it.

[Transcript] Darknet Diaries / 134: Deviant

Who gets to do this and not ever really risk getting hurt for it, you know?

It's, I think it's a great thing to get to do it.

Okay.

I just don't know.

I guess I don't understand the level of like, okay, let's really start light and see how much we can get without even getting a foot on campus or like what.

And some of that is spoken to in terms of the client's willingness to have a more involved job.

I mean, that's labor is cost, right?

So time is money and they provisioned.

They said, no, we're really, they were really serious about, they're targeted by foreign adversaries.

Oh.

They, they, they are targeted by real threat actors at that point.

And an actual threat actor would not think twice about spending an entire night just in belly down in the dirt with long range glass, learning which employees go through which doors at which times and when the security patrols come around and when they don't.

Okay.

So another thing to think about here is this company invested a lot into security.

Cameras all over the buildings inside and out, trip sensors, security teams, they really, really wanted to detect and stop any sabotage or intrusion or disruption against this facility.

And they did everything they could to stop this.

In fact, this company had its own red team who just attacks their own company looking for weak points and vulnerabilities or whatever they could find that an adversary might exploit.

They're on the offense, which makes them a red team.

The defense team is known as the blue team, but it was the head of the red team that hired deviant and his crew.

So he could communicate and confirm certain things

[Transcript] Darknet Diaries / 134: Deviant

with the customer, the head of the red team.
Like for instance, as they were doing the recon,
they noticed something that looked like a radar system
to detect intruders.
So he messaged a client and asked things like,
Keith, are they using spotter RF?
He's like, yeah, you spotted the spotter.
Cool. Yeah.
We have it pretty masked, but you must,
he's like, you must have been really close.
I was like, yeah, we were right up against that fence line.
He's like, okay, yeah, you got it.
You got it.
Don't approach from the west side.
You spotted that one.
Because again, let's say you're the Chinese government
and you got a guy laying in the dirt,
crawling up to a fence line,
and then this guy takes some pictures
and you say, well, look at those technology.
Are they using, oh, oh, that's RF.
They're using spotter RF.
It's a way of looking for motion sensing in a field.
And if it's the Chinese government,
they would then back off and they would say, okay,
let's spend another two weeks figuring out who sold it to them.
Let's figure out which version they have,
what its coverage is.
Whereas for us, we just signal message.
We said, hey, I found this.
Is this what I'm seeing?
They say, no, yeah, yeah.
We're not going to make you charge us
another week's worth of effort to go get a sample unit
and set it up in a lab and figure out
the exact distance and range that it covers.
It doesn't match the manufacturer's spec.
So it's a week of that.
It's a week of getting close, taking pictures,
coming back to the Airbnb, analyzing who's this guard.
Is this mobile too?
No, he was, well, he was on foot yesterday.
No, the guy on foot was in a, okay,
no, this is the guy in the truck.

[Transcript] Darknet Diaries / 134: Deviant

I got, let's make a name for him.

You make up names.

It's like a pinboard, like out of a detective show, right?

You got a wall of people and one really great photo of a guard looking at us through these binoculars.

Yeah, that guy, we printed that photo out a lot, put it around the Airbnb.

So there's some of those guards are really switched on.

Well, cause he couldn't see us, but he saw something and he was like, what's that?

And Robin Drew just stood stock still in the dirt in their ghillie suits for like an hour.

Ghillie suits, those are the big camouflage suits that you see like military use,

where they have like tree branches and leaves sewn into the suit so that you look just like a bush when you're holding still.

Crazy.

Now, of course, they aren't just casing the place physically.

Sophie is also trying to infiltrate the people inside.

She's trying to get pieces of information that could help her know more.

She created a fake social media profile and started trying to connect with people who work there.

The work involved in setting up a fake profile is non-trivial.

It's really hard to create like a fake LinkedIn or a fake anything these days that looks legit.

I mean, you need to have history there.

You need to have connections.

It's like planting crops.

You have to create these profiles and then you water them, you come back

and you connect and you make posts

and you connect to this people

and you endorse that person.

Years later, months and years later, these are now fully formed

and you can maybe use one of them on a job to connect to other people and try to...

But if you get burned, well, that's all right.

There's a year and a half of work that that profile is roasted.

So the fact that she has access to these and she made those connections to find out

[Transcript] Darknet Diaries / 134: Deviant

what was going on and can...
Let's... Can I share your profile
so I can see your photos from the job?
Okay. Now you got the access to the private photos.
Oh, that's the company is having a pizza party on Friday.
That kind of thing.
Okay. So after almost a week of watching
this high security building from the outside,
they determined this place is completely secure.
They found one little area that they could access,
but it was kind of an insignificant finding.
So we determined that it was feasible
to get through the fence line.
In fact, as a proof of concept one night,
a small team did that.
They crawled up to the dirt berm
where the earth had been compacted,
but not quite enough in one spot.
And they trenched under the fence.
They just dug and dug with hand,
like small and trenching tools,
and they're pulling out rocks.
And they proved you could slip under the fence
and they just took a picture of one guy
on the other side of the fence and then came back.
That's not super practical.
We knew this was still a site that was being built out,
and we told our point of contact.
We said, hey, just so you know, we proved we did this.
The shake sensors in the fence didn't catch us.
He said, no, I bet I can tell you
which you probably on the north side,
that's all going to be concreted in.
The footer of the fence is still being built.
We said, okay, well, it's a data point for the metrics,
but we're not going to treat that as a standard entry point.
So the only way to get into this place
was going to be where everyone gets in,
through the vehicle checkpoint.
This place had high fences, barbed wire, cameras,
shake sensors, radar.
It wasn't kidding around,
and that's just to get on the property.
It's like visiting, it was non-military,

[Transcript] Darknet Diaries / 134: Deviant

it was a civilian compound,
but it's like a military base, right?
If you have a working credential,
you drive up to the vehicle checkpoint,
they see it, you boop it, and you go.
If you don't have credentials,
you're going to the visitors building, the tiny shack,
and someone is coming out and dealing with you.
And without a credential, you're not getting in.
But there's always some exploits here, right?
There was some construction going on,
and Deviant was able to drive into the construction area,
just to do some surveillance on the front gate.
He got some good video footage
of exactly how the vehicle checkpoints work.
And we learned, we said, okay, this is interesting,
this is interesting, look at this,
let's look at what happens here.
You drive up, and staff were holding their badge up,
at like, clearly they're presenting a badge to the guard
who visually kind of would nod at it.
Then they would drive further down, a good 10 yards,
past the little overhang, and there was a badge reader
sitting out in the middle of the, just like unattended,
there's just a big badge reader on the,
and they would boop, they would badge that,
and then a vehicle gate, a gate arm would open up.
I said, that's an interesting thing, that's an odd thing.
And then we said, look at that gate arm, look at that gate arm.
Many gate systems will use ground loop sensors,
much like when you pull up to a stop light,
it knows your car is there,
because it can detect the metal of your vehicle,
and it'll cycle the light.
A lot of gate systems use these.
A very typical configuration would be,
the most common one is a stop or safety loop.
Right in where the gate arm is, if a vehicle stalls out
and sits there, for some reason,
the gate arm won't come down and hit the vehicle,
you don't want to damage anything, that's typical.
You might have an entry loop, so that once you pull up,
the gate arm doesn't, you know, just doesn't operate
unless somebody boops their car, like why,

[Transcript] Darknet Diaries / 134: Deviant

you can't walk in on foot, like this is not a pedestrian entrance, I'm sorry, you need a car.

If you're a pedestrian, go to the pedestrian entrance, it's around the fence over there.

This is a very common problem for certain motorcyclists or bicyclists, people on bikes sometimes don't have enough metal to trip the ground loops depending on how they're built, but the real one, and this is the one that a lot of buildings do not use, you got an entry loop, you got that stop loop, the safety loop, there's also sometimes a clear loop, clear meaning you have cleared the checkpoint, bring that arm right down, it costs money to install these, you got to cut into the asphalt and you're doing, you know, everything's money, a lot of installations, this one included, chose to configure it, well, we don't need a clearance loop, we'll just, the arm goes up, there's a dwell time, and after that, it'll just drop down, unless there's somebody stalled out.

So they were using a dwell time, and the dwell time was set to like, gosh, it was like 20 seconds, it was long.

I'm like, okay, this is news we can use.

So our plan was, we're going to tailgate in, we're going to tailgate in behind what we think is a real vehicle, because it was a long entrance road, off the main road, to get even to the vehicle checkpoint.

Our plan was, you're going to tailgate in, we're going to give Sophie in the front seat of the car, who looked business like, we'll give her a badge that looks like their badges, we knew what their badges look like, it's a multinational company, we've seen their badges in other facilities, we don't have their badge technology, they were using private keys on their credentials, so we couldn't easily clone their badges.

But Sophie could pull up and smile at a guard and hold up a badge. Then, because she's tailgating behind someone's vehicle, literally tailgating, as that person boops the reader and goes through, Sophie would pull up, pretend to boop the reader, again, that's 10 yards away from the guard shack,

[Transcript] Darknet Diaries / 134: Deviant

they can't hear a beep noise,
and then before that dwell time finished,
she would hightail it through.
And if a guard was really sharp,
they might be like, that gate came down kind of quickly after that car,
but nobody's gonna be that sharp, we said.
All right, now the critical thing,
we said, we need about three or four,
we need different ways to have you peel off if there's a problem.
The first thing is, there's that construction lot, right,
where I parked, to get the footage,
we said, if for some reason the car you're tailgating
isn't a regular employee,
if anything goes wrong,
if they ask for directions,
they're like, who the hell knows,
just pull into the construction lot,
K-turn and get out of there.
It's a little weird, but who cares,
we'll roast that car, we'll switch the car out,
we'll regroup.
Let's say you're fine, let's say you get past,
like you hold your thing up to the guard,
and the guard looks at you and says, hey,
do you work here, do you not work here, etc.,
you say, no, I'm new here,
so if you're bad, you can social engineer that if you had to.
If you say, oh, I'm lost,
or is this not the main answer to the visit,
no, I just started, okay, well, pull over there, okay,
figure that one out.
The last one was a really slick one,
we said, if for any reason you get trapped at the gate,
like, let's say the arm starts coming down,
and you're like, oh, shoot, I can't tailgate in,
we had printed a nearly identical badge,
it looked very similar,
but the logo was a little different,
it was another company in town,
it was out in the rural area,
but it was another big firm that had a warehouse
or something, a fulfillment warehouse in town,
and we said, pretend to boop and say,
my badge isn't working, my badge,

[Transcript] Darknet Diaries / 134: Deviant

and make the guard get out of the shack and walk over,
but she would switch the badge,
and it was on this red lanyard,
and she's like, my badge isn't,
and so the guard would go, oh,
oh, is this the badge you just showed me?
I'm sorry, ma'am, this is not,
you've got to go down the road another few miles,
you're on the wrong path, oh, I just started,
sorry, so we had all these little outs,
okay, this is a lot of work,
just to get into the parking lot,
Sophie's going to try to drive in,
and it was important that she'd be the only one in the car,
that way the guard doesn't start asking,
like, for passengers to present their badge
and get curious and interested in what's going on,
but through their surveillance,
they noticed the guards never check the trunks of the cars,
it wasn't just her in the car,
it was Robert and I were wedged into the trunk of this car,
because we wanted to get as many people
as we could onto the corporate campus
if we could get this to work,
so they load up their gear,
jam themselves in the trunk,
and off they go, driving towards the facility,
and all we could feel was just the car kind of,
we just kind of rocking back and forth,
and we judge, okay, there's some rough bumps,
those are the speed bumps, okay,
and now we stop for a sec,
that must be the guard shot,
oh, we're moving again, the guard didn't stop her, okay,
and then, okay, we slowed down a little bit,
oh, we're really moving now, that must be the gate arm,
and we're really, we're jitterbugging along for 10 seconds,
20 seconds, we're like, we gotta be through that gate,
we gotta be through, I know we're through that gate,
and we eventually hear Sophie's voice,
like, it's Hollywood, we're through that gate, boys!
Sophie pulls down the back seat,
so the guys can climb through the car,
which will take a while, it's a tight space,

[Transcript] Darknet Diaries / 134: Deviant

and this is where they split up, though.
Sophie goes right to the front door of the building
to try to use her social engineering skills
to get into the building, she was just charming,
she just said, I'm new, she followed a group of people,
I'm new here, I just started this week,
oh, did you get the tour?
She said, no, there was a tour,
we knew that there was a company tour
that somebody posted on social media,
and we're like, well, I didn't get the tour last week,
I heard about that, and this guy who was like,
well, I'll give you the tour, little lady,
so yeah, I mean, he's like, you should check this out,
and he's taking her to a place,
and there were a couple other employees,
one of which even turned and looked at her and went,
hey, I know it's a tour, but you can't tailgate,
you have to use your badge, and she goes, oh, you're right,
and just kind of pretended to boop her badge,
and it's not making a sound, right?
We have little, we've have, you know, beep, beep,
like, on our phones, so if you need to,
everyone's on their phones, so you're just kind of,
oh yeah, beep, beep, and just, okay, then you walk in.
But yeah, that one woman literally said,
are you trying to tailgate?
And she says, oh, you're right, you're right,
they told us this in orientation training,
and then they, but yeah, they took her
into the heart of the beast, right?
She was sending signal messages to all of us,
like, I'm in this thing.
Good pictures.
Oh, good pictures, day one.
Okay, so while she's making her way
into different rooms and getting a solid lay of the land,
deviant and robbed, climb out of the trunk of the car,
and come out of the car.
Climbing out of the trunk directly would be weird,
so they had to sneak through into the car
and then exit through the regular doors to look normal.
Robert and I looked like construction workers.
I mentioned there was construction ongoing at the facility,

[Transcript] Darknet Diaries / 134: Deviant

so we had our sort of jeans and steel cap boots,
we had some high vis, we had, you know,
the helmets kind of clipped to our belts,
if you want to throw a helmet on, you can.
And we had tools, we had workers' tools on us,
and more in the trunk too.
So we just kind of walked around the building
and started, quote, checking doors.
You know, checking the handle is this door really locked,
but also there's a little door gap checker.
It's used, but it's used when I do fire door stuff.
You can, there are tolerances.
This is a quarter inch, eighth inch.
How much tolerance is this door?
You can check at the door jams
in the top of the door, in the bottom of the door.
So we're just, quote, checking doors
and pretending to take notes on a tablet.
And we're going around and seeing
if anybody left door open or could we tailgate in.
And eventually we did.
We tailgated in, we walked through some spaces,
and between us and another team
was able to exploit a similar path.
Now that we know, we're like, well, Sophie got in,
maybe Drew can do it.
Drew is not quite as charming as Sophie,
but Drew can drive through a checkpoint he did.
And Drew was able to tailgate into the building too.
This is where he just waited near a door
until someone was going in or out,
and then he just went in after them
without having to use a badge.
Day one was a success.
All three teams got into sensitive areas
and showed their contact how they got in.
They took photos and were able to leave
without being detected or caught.
So they decided to do it all again the next day.
But this time be a little more sloppy, you know,
like standing near a locked door,
a little more obviously,
and actually looking like you're waiting
for someone to come open it for you.

[Transcript] Darknet Diaries / 134: Deviant

And sure enough, somebody did come open it
and didn't challenge them and held the door open for them.

Or they might have shouted at someone,
hey, can you hold that door open for me?

Thanks.

It was shocking how once we got past that fence line,
we started realizing that no one really challenged us.

Their outer perimeter was very secure,
but it seemed like that was the main layer of defense.

To properly secure a building,
you want to do defense in depth.

And not just one gate at the front,
but many gates the deeper you're going.

And they didn't encounter that.

So now that they've accomplished all their objectives
by getting into all the sensitive areas

that they were tasked to get into,
it was time to step it up a bit or step it down,
depending on how you look at it.

We said, let's just try to be sloppy.

Let's just try to like, hey, buddy, hold that door.

And, you know, don't be polite about it.

And we're like, man, we just keep getting in everywhere.

And we kept getting into so many sensitive rooms.

We were messaging our contacts and we're saying, hey,
you know, we're in here today.

You want us to try the third wear?

You want us to try the this generation building
okay, try to get in that building.

And we're really not getting challenged.

So by the end of the week, you're like, we got,
we really want to give you some wins here.

Do you want us to just start doing stupid shit?

Trying to see what level of noise it would take
to make the employees at the customer site say, hey,
that's not right.

I should report this to security.

And we were setting off alerts and alarms at that point.

We were propping doors open with door stops
that you're not supposed to do.

And if it's held for more than 30 seconds,
then a guard has to come out and go,

why is there a doorstop here?

At this point, we had literally caused headache

[Transcript] Darknet Diaries / 134: Deviant

on the part of the guards because we had been putting door stops in and holding doors open and just really kind of, they were like, what's going on? Why are the employees being such a pain these last 24 hours? This day, at one point, I think I took caution tape and I propped the door open and put caution tape all around the door. And like, just like, do we take the tape off? Do we not? What are they working on? I put a work order on it that's, you know, because we had seen other work orders in maintenance areas. An exit build, like a door? No, this is an internal door to a sensitive machine room. And the guards were like, and they had to escalate to a supervisor and say, no, take the tape down and we'll figure out who left that there later. And we're still not getting quite caught, right? We're still, we were interacting with some guards. I said, hey, who took the tape off this door? That kind of, you know, and but they kept seeing our badges. Okay, so finally we said, what do you want to say? We're on a quick three-way call with the customer. What do you want us to do here, man? We're really trying. We're trying to, we're walking up to people saying, hi, I'm not from this department. Can you tell me where to go? And they didn't know and asked, why are you in here? And they said, well, you said something once about destructive attacks. You can go destructive. What can you do there? You said, could you like, could you like drill a door or something? I was like, I mean, yeah, there are, there are plenty of things we show to other types of entry trainings we do for first responders or for military. We say, yeah, I mean, we could drill a cylinder out of the door and then you take the cylinder out and then you can pop the door. I mean, we can do that. It'll, it'll, it'll be noisy and it'll cause some damage.

[Transcript] Darknet Diaries / 134: Deviant

And they said, yeah, yeah, yeah.
I mean, we'll budget it.
We'll say, here's how much you're allowed to damage
and try to keep it under that amount.
And let's try it on a door or two if you want.
We'll pay for it.
I said, okay.
So we got out of giant, you know,
I actually went to Home Depot or Lowe's or something
and I bought a big old blue Makita hat like hammer drill
with a big handle off the side
and I bought some high speed steel bits.
And there's footage and actually footage
that Robert shot with his cell phone of he and I
in our hive is just
just just carving away at this lock in this door.
And our point of contact was really trying to give
his people a win.
He's in the sock and he's watching and he's watching.
He's looking at his people and he's watching.
Hey, Chris, can you pull up monitor 17?
Can we center stage that for a second and click
in this big screen?
He's like, what's going on outside building six?
Do we have Sheridan here?
Did you see a work order?
Are we service indoors or something on building six today?
I thought that building was already stood up.
And you hear that, you know, like rustling of papers
and they're people like, I thought they had so much work
going on from so many contractors.
They were growing so much at this site
that someone's like, I swear, I swear,
I saw something about that on the pass off notes.
I think we're doing doors.
I think we're doing doors today.
And he's like, okay, and he kind of stepped back
and messaged us and said, no, man,
they're looking at you on camera and you look the part.
What are you going to do?
So yeah, I just kind of dropped the drill where it was left.
The door set off an alarm and I just left the alarm going.
I just walked through, but we were trying everything.
We're just setting off like a chain of alarms.

[Transcript] Darknet Diaries / 134: Deviant

Until guards eventually came to us.
And they said, hey, you know, fellas,
stop what you're doing first.
I was trying to underdoor tool a door
and not hiding it at all.
Just Robert, I stand up and they say,
so what are you guys doing here?
And they're like, were you working on the side of that building six?
I'm like, yeah, yeah, there was like an alarm.
That was really loud.
Like, yeah.
So what are you doing?
What are you doing here, guys?
And Robert again, like back pocket kind of hand on the letter.
Thing and this has got to be our ticket is up.
And I just hail married.
I said, what does it look like we're doing?
And that broke the guard's brain.
He went, well, it looks like you're working on door.
It looks like you're trying to get open this door here,
but you have badges and Robert's hand kind of comes off the letter.
Let's see where this other guys like, yeah, I mean,
if you work here, you're obviously on the contract team,
but you have a radio because Robert had stolen a radio from a truck.
It's like, you can, you know, you can just call for remote unlock.
You don't have to have us come all the way out here and bother with it.
We came all the way from the other side of the thing.
So he's like, yeah, no, it's the Sheridan guys.
I'm here. Yeah, yeah.
And warehouse.
Yeah. Can you open the east side of warehouse?
The door goes green.
He opens the door.
He's like, yeah, see, I mean, you can just do that, man.
You must be, you know, don't worry about it.
But like next time just call, man,
we didn't know what was going on with all these alarms.
I said, oh, thank you.
Yeah. The story continues to get crazier and crazier.
I eventually took a bike because they had corporate,
they had a couple of like people who biked into the corporate office.
I took someone's bike and just biked it around the parking lot,
hoping that someone would report a stolen bike.
I took a golf cart and started driving that around.

[Transcript] Darknet Diaries / 134: Deviant

And they eventually, because again, we had radios. Someone's like, okay, Dive, they're finally onto you. You're going to have some attention soon. And I saw these white pickups with guards start trying to find me in parking lots. They thought I was like a mental case. They were like, is that the same guy? No, he's not wearing the hive is anymore. Who is that guy? And I was just, I was rolling around and there's like, yeah, crazy guys on a bike. No, no, no, no, no, wait, crazy guys in one of our carts. But it distracted them so badly that I had, it was like, it was like an OJ Simpson pursuit. I was pursued by these flashing light vehicles. They couldn't, what are they going to do? Knock me off a bike, try to ram into a golf cart. You can't cause injury. So, and a bike can go places that trucks can't. I would just cut through bushes or cut in between buildings. And then they would have to like spin around and go driving around the other side. And while I was doing that, the other teams knock down every target again and again and again. And they, they took pictures with, you know, standing in all the sensitive rooms because everyone's eyes was suddenly on crazy guy. Yeah, at this point, nobody cared about trying to mask door sensors. It was so many alarms that it eventually was a supervisor who was off site that day. It was his day off. And his phone, his work phone was like lighting up with a light. And he went door 21, door 17, door 17 again, door 17 again, door 55, roll up door 76. He's like, what is going on? And he tried to call, no one would answer. He drove in, he lived in, you know, town over. He drove in, kind of burst through the doors of the security side. He said, what is going the F on? And he's got a bunch of guys. Let's like look into this. This crazy guy is on a bike, sir. He's like, I don't give a damn about that guy.

[Transcript] Darknet Diaries / 134: Deviant

Does he had a parking lot?
What's all this?
And he's looking at all the alerts and they go,
Oh, really?
Something going on.
It's like, look at your screens.
There's all these red entries in the Linnel access.
There's all these failed events.
There's all these door entry events.
He's like, so we heard squawks on the radio
start going out that said mobile six, you watch bike guy.
Everyone else returned to your guard tours,
cancel all superfluous business,
challenge all unknown parties,
figure out what there's more afoot here.
Some guy even said bike guy may be a distraction.
And that's what it took.
That's what it took to finally get them
to start challenging our teams.
And that was at the end,
I just kind of got off the bike at one point
and now these like all these trucks pull up
and they all jump out and like, what are they going to do?
Again, they're not cops.
They're not allowed to shoot your go hands on.
And they went, sir, could you please stop?
And I went, I'm stopped.
I'm perfectly fine.
What's going on, fellas?
Having a good day?
And they asked me to sit down.
I had a lot of seat by the curb.
And I said, this might explain it.
I hand them a letter.
And then some of the guys were former service members.
And they said, oh, all right, it's an exercise.
Boys, look, one of the other teams just got in their car
and left and then security caught the third one
and just asked them, are you supposed to be here?
And they said, no, thanks for asking.
I've been here all week and nobody's asked me that.
With that, their engagement with this client was over.
The client loved hearing all the different ways
that they were able to defeat security that week.

[Transcript] Darknet Diaries / 134: Deviant

And they worked with security to fix all the things that they noticed in their assessment. It was a great training exercise for everyone involved at the facility. Wow. So thank you so much for sharing with us the way you see the world. Yeah, hopefully some people out there start seeing it this way too. It's not a bad way to be. You don't have to live in fear. You just live in awareness. I'm a fan of Amanda Palmer. She is a cool musician and poet. And she talks about how it's not the job of the artist to make you feel joy all the time. It's actually the job of the artist to take you into the darker places. And if you've ever heard her music, she's good at that. But darkness isn't scary because it's dark. It's scary because you're alone. And I like to remind people that if we go into these dark places in our world with friends and allies and peers and loved ones, you realize that the dark isn't that scary because it's dark. It's just because you didn't know it was in there. And that's why I like to bring people into the darkness with me and realize it's not that scary. And they can learn from it and they can be improved by it. A big thank you to Deviant Ola for coming on the show and sharing these stories with us. You should be able to easily find him online by just searching his name pretty much anywhere, Deviant Ola, which is spelled O-L-L-A-M. He's on YouTube, Instagram, Mastodon, Blue Sky, and Twitter. Or you could just look on his own website, which is deviating.net. I'll have all these links in the show notes. Just check the description of this episode. The show is made by me, The Tarnished, Jack Recyder,

[Transcript] Darknet Diaries / 134: Deviant

editing and assembly by The Omen Killer, Tristan Ledger,
mixing by Proximity Sound.

And our theme music is by the dreamlike Breakmaster Cylinder.
And even though the only dates I get are updates,
this is Dark Net Diaries.