[MUSIC PLAYING]

While we all quietly surf around on the internet, an elite of the smartest hackers scans it day and night looking for undetected safety leaks. They convert these secret leaks as if by magic into building blocks for cyberweapons, which they sell for astronomical amounts of money to criminal organizations, but also to security services and cyberarmies, enabling them to infiltrate unnoticed into your computer, banks, or even nuclear plants. Among hackers, there is a gold rush for these lucrative safety leaks, and they call this gold zero days. This is what you're about to see.

If 10 years ago, somebody would have told me that by 2014 it will be commonplace and normal for Western democratic governments do write viruses and Trojans and back doors, that would have sounded like science fiction.

Normally, when you talk about gray and black markets, you're talking about what's legal or illegal. All of this is currently legal. So vulnerability and exploit sales is all currently legal.

In 2007 or 2008 or so, I sold a bug to the US government for something around $50,000 or $80,000.

This is VPRO's *Backlight*-- *Welcome* to *Cyberspace*. For many years, we have admired cyberspace as a magical new world. Enchanted as we were by its infinite online opportunities, we didn't trouble ourselves much about our virtual safety.

While most of us are awakening from that dream thanks to Snowden's revelations, a small online community kept its head over the past 20 years and paid close attention when our digital infrastructure began to develop. A golden age has now begun for hackers who search the internet for zero days, mysterious security leaks that form the raw materials for cyberweapons

On the eve of the biggest hacking conference in the world, DEF CON in Las Vegas, hackers who enjoys shooting as a hobby meet in the desert.

[INAUDIBLE] is it clear?

[GUNFIRE]

Cyberweapons can steal technology, divert politics, get your privacy, learn things about you that they shouldn't know, right now. As the internet of things, to use that term, gets more and more common, the reality of this kind of thing and computer security in general may invade into the physical world. So when we talk about smart cars or linked up cars that have drive by wire systems, braking systems, if they don't do it right, they don't segregate those systems or those things are linked in, the reality of guns being able to kill and cyberweapons being able to kill converge. And I think that we're getting closer and closer to that reality.

By now, we are aware that our personal data, bank information, and online privacy are not entirely safe. But can our physical safety also be hacked in the future? How big is the gap between real guns and hackers who pull the trigger online?

Inside the hat, there's a Wi-Fi router. And if you can log onto the Wi-Fi router and load any web page, it gives you a scoreboard and a list of 40 usernames and password hashes. If you can crack any one of those, you can get on the scoreboard, and you can make the hat say anything that you want.

DEF CON is the largest hacker conference in the world. This is its 22nd year. I think they're expecting 20,000 people this year. And it's a collection of hackers that are good, bad, or indifferent. I know a lot of people think hackers are a menace, but most of us are white hats. In other words, we use our talents and our curiosity and our technical skills to make the world a safer place.

Joshua Corman is a pioneer within the hacking community. He founded I am the Cavalry, a movement that tries to motivate hackers to use their talents to make software safer.

I think this culturally is an early bellwether of where society is going because it's the mash up of fringe culture, technology, and society that show where we're having a bigger impact on geopolitics, on public policy, on safety and things like medical devices, our cars, our homes, our public infrastructure. And what we once did as a hobby is now a critical part of society. And we're only now just figuring this out, and we're starting to act and rise to that sacred responsibility.

Hacking is a form of power. And this new form of power has been solely in the domain of the hacking community for quite some time. They were the early magicians, the early wizards, without really much motivation to use their talents politically or for anything.

The first generation of hackers has come of age. They used to be harmless nerds, but now they're able to completely disrupt society. In the late 1980s, they developed their talents by writing the first malware, software that took over your operating system in an amusing manner. This malware was clearly visible and harmless because it would be gone when you restarted your computer.

Now, 25 years later, our entire society is connected to the internet. Water, energy, and industrial networks all have an IP address, which makes them accessible to hackers. Online safety and physical safety, traditionally separate domains, are slowly beginning to converge. And for the first time ever, malware can now have disastrous consequences.

Our entire power supply can be cut off. Our systems can be taken over. Hospitals deprived of power would cease to function. It's not if. It's when.

[NON-ENGLISH SPEECH]

Ronald Prins is a cryptographer sometimes described as the most powerful nerd in the Netherlands. His company, Fox-IT, provides security for the sensitive information of large companies and encrypts the state secrets of the Dutch government.

[SPEAKING DUTCH]

Young hackers guard the internet and try to detect the truly dangerous malware among the thousands of irregularities.

There is no perfect security. If I could provide you with 100% security, I would. But I can't, so I won't.

Mikko Hypponen is a famous Finnish antivirus expert who travels all over the globe trying to combat malware.

When I started analyzing viruses, it was all just kids writing them for fun. They weren't really getting anything out of it. It was just a challenge. Around 2003, 2004, we started seeing the first money-making malware. That's initially just spammers using botnets to send their spam. So they starting cooperating with malware writers, and that's when these hobbyists started realizing that they can actually use their skills to make money.

And we started seeing this shift of hobbyists starting cooperating with spammers and other online criminals. And in a couple of years, the hobbyists just disappeared. We don't really see them at all anymore. All the malware we see today is written by criminals or hacktivist gangs, or by governments themselves.

Ladies and gentlemen, please give him a warm welcome, Mikko Hypponen.

Thank you for being here today. To speak about governments as malware authors-- if 10 years ago, somebody would have told me that Western democratic governments will create offensive malware and deploy it against other democratic, Western, friendly governments, that would have sounded like science fiction. Yet, that's exactly what's happening today-- for example, UK intelligence launching offensive malware attacks against Belgian telcos, which happened.

We probably wouldn't have guessed how active governments would have become by 2014 writing active offensive malware for computers and phones and tablets that we use all the time.

A real-time visualization of the biggest malware attacks happening in cyberspace, a world war fought with ones and zeros. As long as we assume that these attacks have no physical consequences, maps like these look like a computer game. But in 2010, it became clear that some of these colored lines can be powerful weapons with consequences in the real world.

In June last year, a computer virus called Stuxnet was discovered lurking in the data banks of power plants, traffic control systems, and factories around the world. 20 times more complex than any previous virus code, it had an array of capabilities-- among them, the ability to turn up the pressure inside nuclear reactors or switch off oil pipelines. And Stuxnet could tell the system operators everything was normal.

What was it looking to shut down? The centrifuges that spin nuclear material at Iran's enrichment facilities. Stuxnet was a weapon, the first to be made entirely out of code.

[SPEAKING DUTCH]

Last year, the Dutch Army started to train cybersoldiers in order to be able to defend and attack in cyberspace.

[SPEAKING DUTCH]

We may not have seen a real cyberwar yet, but it's not unthinkable that one may occur in the near future.

Critical infrastructure is exposed. So if you wanted to shut off the power in a city, or if you wanted to cause traffic mayhem, you can have damage like you saw with the centrifuges in the Iranian facility through Stuxnet. It's not going to have the same blast as a nuclear weapon. That would be a horrible false equivalence, but it's so pervasively deployed that one can disrupt those things. The bottom line is we're putting so much vulnerable, hackable, connected technology into so many places, that this makes us prone to the willpower of any potential adversary or foe.

The nature of this domain, the nature of cyber, so to speak, is offense is really easy, really easy, and defense is really hard. So if you were in a sporting event where you could score a lot of goals but you couldn't defend many goals, think World Cup but with a very high score, it's your biological prerogative, it's your imperative to get really, really good at scoring goals. So I'm looking at this less more moralistically, and just the nature of that battlefield favors offence.

It's abstracted, right, from the reality of what it is. It's a lot different than, gosh, just seven years ago when a pilot was doing his thing, he was seeing what he was doing. Or if you were a soldier on the ground firing a rifle, you're pretty much seeing what you're engaging, to a degree.

It's changing in the physical realm, but in the cyberworld, too. I mean, we don't know what's out there. Flame as malware, the Flame malware that affected Windows, that went for five years undetected. What's going undetected now? I can't answer that. We don't know. It's undetected.

Cyberspace is like the Wild West with malware roaming around undetected. This invisible evil can damage our computers undisturbed because they are full of security leaks. Top hackers look for undetected security leaks, zero days, extremely valuable security leaks that have been known for zero days, meaning that not a single security person will yet know of their existence.

Hackers can exploit zero days as if they were digital pass keys, giving them access to your computer or your bank or even to a nuclear power station without anyone noticing. Once inside, they can install any malware they like without alerting the system. It is estimated that Stuxnet, the attack on Iranian nuclear centrifuges, used as many as 20 zero day exploits.

[SPEAKING DUTCH]

Back in the beginning, security researchers could only ever expect an acknowledgement or credit from the vendor for finding a vulnerability and reporting it to them and letting the vendor fix it. And that credit actually was a form of currency. That recognition was something that security researchers could use to leverage to build a career and get money that way. And then it became replaced by direct monetary compensation for bugs.

We know that software is always going to have vulnerabilities. As long as humans write code, there will be flaws in code.

So when I look at the vulnerability and exploit market, I look at it in terms of white, gray, and black market. And normally, when you talk about gray and black markets, you're talking about what's legal or illegal. All of this is currently legal. So vulnerability and exploit sales is all currently legal.

So white market, they buy vulnerabilities in order to use them for defensive purposes. Typically, it's either the vendor themselves paying for it or a broker who will share it with the vendor at no cost to try and get it fixed, to try and protect people. That's white market, and the prices are typically lower than the other two markets.

Gray market can be mixed use. So some of the stuff is sold as vulnerability information services. Some of the stuff is sold as ready-made exploit kits, what we call weaponized exploits. And those are obviously going to be used for attack. And then the black market, solely for offensive purposes, and those pay the highest prices.

You guys want to talk about exploit sales?

No.

Let's take it over to exploit sales, man.

Why, do you want to buy some?

Yeah, where do I buy some? Let's start with that. Like, where do you buy some exploits, man?

EBay.

EBay.

[LAUGHTER]

I'm actually not going to talk about exploit sales at all.

Why not?

Because we lack an idiot to--

White, gray, black, that's all here in the same room?

Oh, absolutely.

Hacker Katie Moussouris is an important player on the white market for zero day exploits. She works for HackerOne, where white-hat hackers can register their exploits in exchange for prize money, so-called bug bounties, which have lately risen to serious amounts of money. Internet companies hope thus to keep white-hat hackers on the straight and narrow, making the internet safer.

And the winner gets $200,000 for his idea.

One successful, young, white-hat hacker is 17-year-old Oliver Beg. He made thousands of dollars by finding zero days for Yahoo. Oliver also hacks Dutch banks with some regularity, and he hacked the Dutch tax office.

[SPEAKING DUTCH]

One site had an online shopping basket with a discount coupon. Oliver detected a zero day in the underlying code and discovered a faulty input which reduced his bill to no dollars at all. He could have shopped for free, but instead he sent this video clip to Yahoo to help them resolve this vulnerability.

[SPEAKING DUTCH]

Oliver finds zero days in big websites. For hackers, the next level is finding zero days in well-known software that everyone works with, for example, your operating system or your internet browser.

[SPEAKING DUTCH]

In terms of, you know, the broadest sense of those who are capable of finding some of the simpler vulnerabilities, like web vulnerabilities, there are tens of thousands of those types of researchers in the world. But the researchers who can bypass platform-wide shields, there are probably about a thousand individuals worldwide who know how to do that kind of thing on modern operating systems and software. Of that thousand, there's less than half who are willing or capable of working alongside the good guys and the vendors and the defenders. So it's a very thin market when you're trying to attract those types of researchers to either work for you or, in the case of white market bug bounty programs, if you're trying to attract them to sell their vulnerabilities and exploit techniques to you.

There is a worldwide elite of an estimated 1,000 hackers that may be white hat or black hat. They mingle once a year in Las Vegas at parties sponsored by large internet companies. This is where we meet a former cryptographer of the American intelligence service, NSA. He hacked the first iPhone and MacBook Air. Charlie Miller, he's an authority when it comes to zero day exploits.

If I can make your computer send me an email with all your photos, like, I've won. You can't argue that I didn't do it, right? So that's what I think is fun about it. There's no gray. Like, I've either hacked you, or I haven't. And if I can do it, I can prove it to you, and then you have to listen to me. And so that's one of the reasons I like about it.

But it's not as exciting as you would think because it takes maybe a month of work, and you're always getting closer and closer and closer. And at some point, you know you're going to win. You know you're going to succeed. It's just a matter of time. And so when that comes, like, you're happy to be done. But you knew it was coming, so it's not like, oh, my God. It's not like TV where, OK, oh, I'm in. That's not how hacking works. Hacking is days and weeks of effort, and then eventually it all adds up and you get in.

There's lots of ways to find vulnerabilities in software. The easiest way, and the way I prefer, is called fuzzing. And what that means is you just send lots and lots of inputs into a program, and the program should say things like, oh, that's invalid. So you're sending invalid inputs. And it says, that's invalid, or I can't deal with that, or whatever. What it shouldn't do is just fall over dead.

But if you send a lot, a lot, a lot of inputs into it, sometimes will fall over dead. And maybe that only happens one in a million times, which is very rare. But if you're sending 100 million inputs, it happens quite a bit. And so it's just a matter of scale. So if you send enough inputs that are crafted horribly, eventually the program fails. And sometimes it fails in an innocent way, but sometimes it fails in a security-important way.

And so you have to just fuzz for a long time, you know, days, weeks, months, whatever. You just have a bunch of computers running. And you wake up every day, and you look at them. And you're like, hey, look. Nothing happened. But every once in a while, you're like, oh, my God, look what it found.

So I have this funny graph I show sometimes where it's just my electricity bill. And you can see my electricity bill is a certain amount, and then I turned on my fuzzers. And it goes way up because I have all these computers running all the time very hard.

There's a huge demand for hackers capable of finding complex zero days. They can offer their services to the white, gray, or black markets. All three markets are legal. What ethics do they use in making their choice?

I'm entirely fine if people want to, like, sell exploits to the military. But even, is it is misused? Are the sellers or the finders or the researchers then responsible for that? Like, we sold it. But if you use it in violation of international law, or if you use it in violation of moral principle, how is that suddenly my fault?

You got five minutes-- three minutes?

Yeah, I got three minutes.

OK, so you want to give your name, or no?

Sure, I'm Dan.

OK.

So, Dan, we're talking about hacking culture. What are the motives of hacking? They originally wanted to talk about the ethics of, you know, should you be selling weaponized exploits to the government. What kind of changes are we making? And what kind of changes should we be making?

Well--

You don't have to be political.

No, no, it's a scale game, right, because on one side you say, if I have an O day, I can sell this O day for $500,000. Or I can sell it for a million dollars. When you're dealing with those sums of money, people's motives change because if I told you I want you to crack into the NSA for me, here's $5, you'd say, you're retarded. Go away.

If I said I want you to crack into the NSA, I have a dump truck full of gold for you, you might reconsider. You're like, dump truck full of gold-- I could probably get away with a lot of things if I had a dump truck full of gold. So things get gray very quick when you take the amount of money that people are passing back and forth into consideration.

People are going to sell bugs. It doesn't matter how many people you hate for doing it or if you decide they're all evil. Like, you're not going to stop them by thinking they're evil. So in the same way that people will sell arms and people will kill each other as long as they want to kill each other, bugs are going to exist. People are going to sell bugs. I mean, the way I sometimes describe the community is this is the community of people who would very willingly research nuclear fission knowing that they're going to produce the nuclear bomb because they know that fission is cool for totally other reasons. And they've very much come to terms with that side of things, I suppose.

How to make the majority defend us?

Well, I mean, thus far, and you've walked around the halls of DEF CON, very few have figured out the geopolitical power they have or the role that they could play in things like this. The awakening hasn't happened yet.

Now, they were very motivated last year right after the Snowden leaks. They were very concerned about censorship and surveillance, and some of them were building new tools to have more secure and private anonymous conversations. But that's still the vast minority.

I guess I sometimes think about this in terms of comic books, like the mutants in the X-Men. The X-Men were formed to have a positive, constructive use of their power, and Magneto formed the Brotherhood of Mutants to be the next step of evolution passed humans. And without getting into too much comic book lore, I think one reason that I'm motivated to do I Am the Cavalry is to give a positive, constructive use of our mutant powers, so to speak, because the alternative could be worse.

Hackers have power, and Joshua wants to use this power to the good by motivating hackers to make not only software safer, but also things like medical equipment, airplanes, and cars.

Good morning.

Good morning.

So really what's stuck in it with us and really works in the Beltway and with policymakers and the general public is the simple truth, the immutable truth that our dependence on technology is growing faster than our ability to secure it. We want to ensure that the technologies with potential impact on public safety and human life are worthy of trust. It doesn't mean we can go fix them, but we're going to do what we can with our power, with our talent, with our power of story and research and by teaming with industry to make sure that we can achieve these goals.

That's OK, but did you like the Glock, right?

Yeah, I know.

I think you'll like the bullpup, too. It's nice.

But it's pretty heavy.

Yeah, and it's pretty loud, but it actually doesn't have much of a kick to it.

Not a hardrecoil.

No, it's not a very hard recoil at all. My wife fired my Glock 40, and she liked it. But then she fired a 45, and she fell in love with the 45. So she's got one, a 45, already.

The philosophical side is being it's computer security, there's always this arms race. We're fighting the bad guys or the good guys, and it's not always clear which one's the good guy or the bad guy. But with technology and computers, the technology itself is neutral. It doesn't do anything. It's what you do with it that determines the bad or the good.

Guns are no different. They're physical objects. They can launch projectiles at high speed. They can be used for good or for bad. You could defend yourself. You could hunt for food. You could do something awful, which we've seen in the news. Or you could be a government and do lots of awful things in recent history with them. But without them, you're definitely defenseless against any of it. And that means not just computers and technology and the internet, but in my opinion, guns, too.

[SPEAKING DUTCH]

Zero days are controversial building blocks used by ministries of defense and intelligence services to install monitoring software and build cyberweapons. There is a curious paradox in cyberspace. For a safer world, security leaks are used that keep our software unsafe.

So one thing the governmental malware writing has created is a market for vulnerabilities and exploits and zero days because governmental attackers need a way to jump from the net to the target systems. And since they are unable to create enough exploits by themselves, they are outsourcing that exploit development to other parties, third parties, including defense contractors, but also these small boutique companies that do nothing else than create vulnerabilities or find vulnerabilities and create exploits for them, weaponize those exploits, and then sell them to different governments.

How big is this industry?

Nobody know for sure how big it is. It's clearly in the tens of millions globally every year. We know that just looking at their price lists, some of which we have.

This is an exploit subscription service where they guarantee to you at least 25 zero days a year at the price of $2 and 1/2 million. That's a good deal, I'm sure.

A worldwide IT security industry meets the needs of governments to control the digital domain. It supplies complex products in which zero days play an important role. One of the most controversial businesses is Vupen, a French company that openly conducts a trade in zero day exploits.

There's no guarantee that once you sell the exploit, it's only being used for certain things. I mean, that doesn't worry you?

Well, it doesn't worry me because it's not true. Exploits do not kill. Computers do not kill. If a repressive regime wants to kill people, they have old-school methods. So they don't need zero day exploits.

So I worked for the NSA for five years back in 2000, 20005. And even though I really have no idea what's going on there anymore, I can't really talk about governments and exploits and that sort of thing.

Yeah, OK, you signed for that, or?

What's that?

You signed for that, not talking about that?

Well, not specifically that, but I can't talk about anything even closely related to what I did when I worked in the NSA.

Yeah, OK, but have you sold to government?

What's that?

Have you sold to government?

Yes, in 2007 or '08 or so, I sold a bug to the US government for something around $50,000 or $80,000. And I wrote a paper about it because I thought-- now, everyone kind of knows that that happens, but at the time no one talked about it. And so for me, I thought it was important to sort of get it out in the open that, hey, there's this issue where people are finding bugs and selling them and making money.

But they're not getting fixed. So I wanted to at least get that out there. So I wrote this paper about it and talked all about all the processes I went through with the bug and how it didn't get fixed for a long time and all this kind of stuff.

What is your opinion, then, on many companies being regarded as controversial, like Vupen, Endgame, all in that market? Do you have an ethical standpoint about that?

Not really-- I mean, I think if we want to put Vupen out of business, what we need to do is make secure software. If they can't hack our stuff, they can't sell anything. And so Vupen is a distraction. Don't worry about them. They're going to do their thing. But if we do our job, writing secure software, we'll put them out of business just naturally. So let's focus on that.

One simple solution for all online threats would be to manufacture truly safe software. We try to achieve this by constantly updating our smartphones, tablets, and computers. Although the authorities encourage this, such security updates also pose a problem to them because truly safe software inevitably means a loss of detection possibilities. In order to enable nations to hack, some security companies play a cat and mouse game with the big software suppliers.

You have new challenges today. Sensitive data is transmitted over encrypted channels. Often, the information you want is not transmitted at all. Your target may be outside your monitoring domain. Is passive monitoring enough? You need more. You want to look through your target's eyes. You have to hack yourtarget.

Let's say the device is a computer. You'd be able to see all of the key strokes that the operator used. You'd be able to go into their memory, find out what documents were stored there, what information is available on that machine. If they used Skype, you'd be able to monitor that call. You'd be able to turn on the camera or the microphone when the subject was unaware of it and hear and see what was going on in front of the computer.

All of those kinds of capabilities. So it's a very powerful system. And as I say, I recognize that a lot people find that to be perhaps frightening, but it's also a capability that's available from other-- to the bad guys. It can be done not just by us. It's available on various black internet sites that provide these kinds of capabilities to criminals and terrorists.

And if it's installed on my device, I will not find out?

That's certainly the objective of Hacking Team to make sure that whoever is the subject of the investigation is unaware that it's being used against them.

In addition to surveillance software that operates invisibly on your computer, the IT security industry also offers fuzzers to governments, expensive software that can trace zero days automatically while your antivirus software gropes around in the dark.

As a consumer, I think I make myself very secure by using an antivirus program. What's the difference with such a program?

Well, antivirus programs, they try to stop known vulnerabilities. Well, if I'm a hacker, and I don't want to be discovered, I'm not going to use a known vulnerability. I'm going to use an unknown vulnerability and write an exploit. So we find the stuff the hackers use to find unknown vulnerabilities and write zero day exploits that nobody knows about until somebody finds them.

Do you have a sort of ethical code to who you sell?

Yeah, I mean, we sell to large companies, governments, militaries that want to protect their command and control networks, critical infrastructure. So we just don't sell to some random hacker that tries to come to us. So we vet the customers, but most of them are very large organizations.

But I mean, could military or intelligence use your product to develop offensive products?

They could. The stuff we find is really the raw material of cyberweapons.

If I want to buy the full package, what are we talking about?

I mean, if you want to buy all the stuff we have to test everything, you're probably talking 2 million euros, around, a little plus or minus, probably a little bit more plus.

We are in the middle of a cyber arms race. Any military that has any kind of capability is right now stockpiling capability for launching cyberattacks in case they need that in future crises. And in that sense, we are in the middle of a cyber cold war, if you will.

I don't think the internet can be controlled, and I fear that the attempt to do so will only make things worse. You're here at DEF CON, the largest hacker conference in the world. And no matter what people do to try to control it, there will always be a way to undermine it.

The minister of security and justice in the Netherlands, Mr. Ivo Opstelten, Minister.

That society must be able to enjoy the full benefits of the digital age safely.

We need to collaborate. Only together with our partners we can ensure that the Netherlands is safe and remains safe, offline and online.

[SPEAKING DUTCH]

The conversation needs to start to turn to what's the role of government in protecting its citizens. Things could get very ugly very quickly. And that's one of the reasons I'm trying to advance focus not on the weapons or the zero days or the techniques or offense or defense, but the bigger picture of, what should the new social contract be? Cyberspace has no clean boundaries, no clean jurisdictions, and probably never will. It's an existential threat to the nation state.

Nations are fighting for control of cyberspace, making large-scale investments in surveillance and cyberweapons. What role do we want our governments to play online if at the same time they have a vested interest in security leaks? And how can we, as citizens, organize our own cybersecurity?

So we need you to help out. We need you to understand that it isn't all about building the coolest tool. It's sometimes about building the coolest tool and helping other people out, or building the coolest tool and understanding that, hey, this neat thing that gives us privacy or that neat, awesome, new encryption platform, it not only lets us encrypt our emails with each other, but it helps the person on the other side of the world, the activist, the person who's trying save their country, trying to make change.

[MUSIC PLAYING]