MY WEIRD PROMPTS

Podcast Transcript

EPISODE #381

The Invisible Hack: The Rise of Zero-Click Exploits

Published January 30, 2026 • Runtime: 27:12

https://myweirdprompts.com/episode/zero-click-exploit-security/

EPISODE SYNOPSIS

What happens when the "weakest link" in cybersecurity—the human—is removed from the equation entirely? In this episode, Herman and Corn dive into the sophisticated world of zero-click exploits, where a single incoming message can compromise your device without you ever knowing. They break down the technical wizardry of Pegasus spyware, the multi-million dollar market for zero-day vulnerabilities, and why legacy code from the 1990s still poses a threat to modern smartphones.

DANIEL'S PROMPT

Daniel

Hi Hermann and Coran. We've often discussed the tiered approach to cybersecurity and how the human operator is often the weakest link. However, zero-click exploits, such as the Pegasus spyware from the NSO Group, bypass that human layer entirely because they don't require any user interaction. These exploits can inject malware through apps like WhatsApp or SMS without the user ever knowing. How can individuals, especially high-profile targets, protect themselves against these sophisticated attacks? Let's talk about zero-click exploits in today's episode.

TRANSCRIPT

Corn

Imagine you are sitting at home, your phone is on the table, and you are not even touching it. It is Friday, January thirtieth, twenty twenty-six. You have not clicked any suspicious links, you have not opened any strange emails, and you certainly have not downloaded any shady apps. But as you sit there, someone thousands of miles away is currently scrolling through your photos, reading your encrypted messages, and even listening to you through your own microphone. It sounds like something out of a spy novel, but for many people around the world, this is a very real and terrifying reality.

Herman

It really is the ultimate nightmare scenario for anyone who cares about privacy, Corn. I am Herman Poppleberry, and today we are diving into one of the most sophisticated and unsettling topics in the world of cybersecurity. Our housemate Daniel sent us a voice note about this earlier today, and it really got us thinking about the shift from traditional hacking to these silent, invisible attacks.

Corn

Yeah, Daniel was asking about the human element, right? We often talk about how the person using the device is the weakest link. You know, the one who clicks the link they should not have. But what happens when you remove the human from the equation entirely? Today we are talking about zero-click exploits.

Herman

That is the crucial distinction. In the industry, we have spent decades training people to be vigilant. Do not click that link. Check the sender's email address. Look for the padlock icon. All of that advice is based on the idea of a one-click exploit, where the attacker needs the victim to perform some kind of action to let them in. It is like a vampire that needs to be invited across the threshold. But a zero-click exploit? That is a vampire that can just walk through the wall.

Corn

It is a complete paradigm shift. And when we talk about this, the name that always comes up is the NSO Group and their Pegasus spyware. We have seen reports about this for years now, but I think the sheer technical brilliance, and the sheer malice, behind how it works is still hard for most people to wrap their heads around.

Herman

It really is. To understand why zero-click exploits are so effective, you have to look at how our phones actually process information. Every time you receive a text message, or a WhatsApp notification, or even an image file, your phone has to do something called parsing. Basically, the operating system or the app has to look at that data and figure out what it is so it can show it to you.

Corn

Right, so even before I see the notification on my screen, the phone has already started processing that incoming data.

Herman

Exactly. And that is where the vulnerability lives. If an attacker can craft a very specific, very malformed piece of data, they can trick the software that is doing the parsing. It is often a memory corruption issue. They send a message that says, hey, here is a tiny image file, but the file actually contains instructions that tell the phone's memory to overflow and start executing a different set of commands.

Corn

So the phone is essentially hacking itself before the user even knows a message has arrived?

Herman

In many cases, yes. With some of the most famous Pegasus attacks, the victim would receive a message through iMessage or WhatsApp, and the exploit would trigger immediately. The attacker could even set it up so the message would delete itself right after the infection. The user would never see a notification, never see a message, and never have any reason to suspect their device had been compromised.

Corn

That is what makes it so different from the stuff we usually talk about. Most cybersecurity is built on layers of defense, but if the very first layer, the way the device handles incoming data, is compromised, everything else can fall like a house of cards.

Herman

It is incredibly difficult to defend against because it targets the core functionality of the device. You cannot just tell people to stop receiving messages. That is the whole point of a phone.

Corn

I remember reading about the FORCEDENTRY exploit that was used to deliver Pegasus. That one was particularly wild because it used a vulnerability in how Apple's systems processed PDF files and images.

Herman

Oh, that was a masterpiece of dark engineering. They used a very old, very obscure image compression standard from the nineteen-nineties called JBIG2. Most people have never even heard of it, but it was still supported by the system for compatibility reasons. The attackers realized they could use that old code to build a virtual computer inside the phone's memory and then use that virtual computer to bypass all the modern security protections.

Corn

It is amazing how these old, dusty corners of code can become the biggest vulnerabilities. We always think of technology as being this cutting-edge thing, but it is really a massive pile of legacy systems stacked on top of each other.

Herman

That is exactly right. And because modern smartphones are so complex, the attack surface is just enormous. Think about how many different types of files your phone can open. How many different protocols it uses to talk to the internet. Every single one of those is a potential doorway for a zero-click exploit.

Corn

So, if these attacks are so sophisticated and so hard to detect, who is actually using them? Because this does not sound like the kind of thing your average script kiddie is pulling off in their basement.

Herman

No, not at all. These are what we call state-grade cyber-weapons. Developing a reliable zero-click exploit requires a level of expertise and resources that very few organizations possess. We are talking about teams of elite researchers working for months or years to find a single vulnerability.

Corn

And then they sell that vulnerability to companies like the NSO Group, or they are developed by companies like that directly.

Herman

Right. And companies like NSO Group then sell the finished product, the spyware like Pegasus, to governments around the world. They claim it is for fighting terrorism and serious crime, but as we have seen from numerous investigations, it is frequently used to target journalists, human rights activists, and political opponents.

Corn

This brings up a really interesting point about the business of zero-day vulnerabilities. For those who might not be familiar with the term, a zero-day is a vulnerability that the software manufacturer, like Apple or Google, does not know about yet. So they have had zero days to fix it.

Herman

And the market for these is absolutely massive. A reliable zero-click, zero-day exploit for an iPhone can be worth millions of dollars on the private market. There are literally companies whose entire business model is finding these holes and selling them to the highest bidder, which is usually a government agency.

Corn

It is a literal arms race. On one side, you have the tech giants like Apple and Google who are trying to make their devices as secure as possible. They have some of the best security engineers in the world. And on the other side, you have these private companies and state actors who are incentivized to find the one tiny crack in the armor.

Herman

And the scary thing is that the attackers only have to be right once. The defenders have to be right every single time, across millions of lines of code.

Corn

I think a lot of people listening might be thinking, okay, this sounds bad, but I am not a head of state. I am not a famous journalist. Why should I care about zero-click exploits? Is this something that could actually affect the average person?

Herman

That is a great question, and it is something we should really dig into. While it is true that these specific, multi-million dollar exploits are currently used for highly targeted attacks, the history of technology shows us that what is cutting-edge today becomes commonplace tomorrow.

Corn

Right, the "trickle-down" effect of malware.

Herman

Exactly. Once a certain type of attack is proven to work, other groups start looking for similar vulnerabilities. The techniques get refined, the tools get easier to use, and eventually, you start seeing these kinds of exploits being used by less sophisticated criminal organizations for things like identity theft or financial fraud.

Corn

Plus, there is the issue of collateral damage. If a government uses a zero-click exploit to target one person, but that exploit relies on a flaw in an app that billions of people use, then every single person using that app is technically at risk until the flaw is patched.

Herman

And we have seen cases where these tools leak. Remember the EternalBlue exploit? That was a tool developed by the National Security Agency in the United States. It was stolen and leaked by a group called the Shadow Brokers, and then it was used to power the WannaCry ransomware attack that crippled hospitals and businesses all over the world.

Corn

That is a perfect example. A state-level weapon became a global epidemic almost overnight. So, even if you are not a high-profile target, the existence of these vulnerabilities makes the entire digital ecosystem less safe for everyone.

Herman

It also changes how we have to think about trust. If you can be hacked just by receiving a message, even if you do not open it, how can you ever really trust that your device is secure?

Corn

It really undermines the whole idea of end-to-end encryption, too. I mean, WhatsApp and iMessage are encrypted, which is great for preventing people from intercepting your messages while they are in transit. But if the attacker can just take over the device itself, the encryption does not matter because they are reading the messages right off the screen.

Herman

That is the big misconception. People think encryption is a magic shield. But encryption only protects the data while it is moving. Once it lands on your phone and gets decrypted so you can read it, it is vulnerable if the phone's operating system has been compromised.

Corn

So, let's talk about what can actually be done. If the human element is bypassed, what are the technical defenses? I know Apple introduced something called Lockdown Mode recently. Is that a response to this?

Herman

It is a direct response to the Pegasus and zero-click threat. Lockdown Mode is basically a nuclear option for your phone's security. When you turn it on, it drastically reduces the attack surface by disabling a lot of the features that are commonly exploited.

Corn

Like what? What does it actually turn off?

Herman

It blocks most message attachment types other than images. It disables link previews. It turns off certain complex web technologies that can be used for attacks. It even blocks incoming FaceTime calls from people you have not called before. It basically turns your high-tech, do-everything smartphone into a much simpler, much more restricted device.

Corn

It sounds like it makes the phone a lot less fun to use.

Herman

It definitely does. It is not something the average person would want to have on all the time. But for someone like a journalist working in a hostile environment, or a political dissident, the trade-off is worth it. It is about making the cost of an attack so high that it is no longer worth it for the attacker.

Corn

I think that is a key concept in security—increasing the cost of the attack. You can never make anything one hundred percent secure, but you can make it so difficult and so expensive to hack you that most attackers will just give up and look for an easier target.

Herman

Right. And it is not just about the cost in money, but also the cost in terms of burning their assets. If an attacker uses a multi-million dollar zero-click exploit and it gets detected because the target was using Lockdown Mode, that exploit is now useless. The manufacturer will patch it, and the attacker has just lost their very expensive tool.

Corn

That is why these groups are so careful about who they target. They do not want to use their best stuff on someone who might be looking for it.

Herman

Exactly. It is a game of shadows. But there are things that even non-high-profile people can do to protect themselves, and I think we should go over those. It is not just about Lockdown Mode.

Corn

Well, the most obvious one, and we say this all the time, is updates. But in the context of zero-click exploits, updates are even more critical, right?

Herman

They are the absolute most important thing. When a company like Apple or Google finds out about one of these flaws, they race to patch it. If you are running an old version of your operating system, you are essentially leaving your front door unlocked. Many of the most famous Pegasus attacks relied on vulnerabilities that had already been patched in newer versions of the software.

Corn

So, if you get that notification that an update is available, do not hit "remind me later" for three weeks. Do it now.

Herman

Do it immediately. Another thing is to be mindful of the apps you use. Some apps are more secure than others. Apps like Signal, for example, have a very strong focus on security and a smaller attack surface than something like Facebook Messenger.

Corn

And what about the idea of "rebooting" your phone? I have heard that some of these exploits are not persistent, meaning they disappear if the phone is turned off and on again.

Herman

That is actually true for a lot of modern mobile malware. Because of the way iPhones and Android phones are designed, it is very hard for a piece of malware to "stay" on the device after a reboot without being detected. So, many attackers choose to keep the malware in the phone's temporary memory.

Corn

So, simply turning your phone off and on once a day could actually kick out an attacker?

Herman

It might not prevent the initial infection, but it can limit how long they have access. It forces them to re-infect the device, which increases the chance that they will be caught. It is a simple habit that can actually make a big difference.

Corn

It is interesting how such a low-tech solution can help against such a high-tech attack. What about hardware? We have talked in the past about things like the PinePhone or other privacy-focused hardware. Do they offer any protection against zero-click attacks?

Herman

They can, primarily because they are less common. Attackers focus their resources on the systems that most people use, like iOS and Android. If you are using a niche operating system, you are a much less attractive target because the exploit someone developed for an iPhone will not work on your device.

Corn

Security through obscurity?

Herman

To some extent, yes. But also, some of those devices have physical kill switches for things like the microphone and camera. Even if someone hacks the software, they cannot turn on the microphone if you have physically disconnected it with a switch.

Corn

That is the ultimate peace of mind, I guess. But for most of us, that is not really practical. We are stuck with our iPhones and our Pixels.

Herman

And for the vast majority of people, those devices are incredibly secure. We should not lose sight of that. The reason these zero-click exploits are so expensive and so rare is because the baseline security of our phones is actually very good.

Corn

That is a fair point. We are talking about the extreme edge cases here. But it is important to understand those edge cases because they show us where the vulnerabilities are.

Herman

It also highlights the importance of the work being done by security researchers. Groups like Citizen Lab at the University of Toronto have done incredible work in uncovering these attacks and holding companies like NSO Group accountable.

Corn

They are like the investigative journalists of the digital world. They find the evidence of these attacks, they reverse-engineer them, and they let the world know what is happening. Without them, we would be completely in the dark about most of this.

Herman

I think this also brings up a bigger conversation about regulation. Should companies be allowed to sell these kinds of cyber-weapons? And what kind of oversight should there be for the governments that buy them?

Corn

That is a massive question. We have seen some movement on that front recently. The United States government, for example, put NSO Group on a blacklist, which makes it much harder for them to do business with American companies.

Herman

And there is ongoing litigation. Apple and WhatsApp have both sued NSO Group for exploiting their platforms. It is a sign that the tech giants are starting to fight back against the companies that are undermining their security.

Corn

It is a weird situation where the tech companies are essentially acting as a form of global governance because they are the only ones with the power to actually push back against these actors.

Herman

It really is. When Apple releases a security update, they are protecting millions of people all over the world, regardless of what country they live in or what government they are under. In a way, they are providing a form of digital sovereignty.

Corn

But that also gives them an incredible amount of power. We are essentially trusting these massive corporations to be the guardians of our privacy.

Herman

And that is a whole other episode, Corn. But for today, I think the main takeaway for our listeners is that while zero-click exploits are a serious and growing threat, they are not something to be paralyzed by.

Corn

Right. It is about being aware, staying updated, and understanding the risks. If you are someone who might be a high-profile target, take the extra steps. Use Lockdown Mode. Be careful about what apps you use. And for everyone else, just keep those devices updated and maybe give them a reboot every now and then.

Herman

Exactly. Knowledge is the first step in defense. The more we understand how these things work, the better prepared we are to deal with them.

Corn

I also think it is worth mentioning that even though the human element is bypassed in the exploit itself, it is still very much a human problem. These tools are created by humans, used by humans, and targeted at humans.

Herman

That is a profound point. The technology is just a tool. The real issue is the intent behind it. And that is why the work of activists and researchers is so important—to shine a light on that intent and demand accountability.

Corn

We have covered a lot of ground today, from the technical details of memory corruption to the global politics of cyber-warfare. It is a lot to take in.

Herman

It really is. But I think it is one of the most important conversations we can have right now. Our digital lives are becoming more and more integrated with our physical lives, and the security of one is inseparable from the security of the other.

Corn

Well, before we wrap up, I want to remind everyone that if you are finding these deep dives helpful, please take a moment to leave us a review on your podcast app or on Spotify. It really helps the show reach more people who might be interested in these topics.

Herman

Yeah, we genuinely appreciate the support. It is what keeps us going. And if you have questions or topics you want us to explore, you can always get in touch through our website at myweirdprompts dot com. We have a contact form there, and you can also find the RSS feed for the show.

Corn

And a big thanks to our housemate Daniel for sending in this prompt. It was a great one to dig into.

Herman

Definitely. He always keeps us on our toes.

Corn

So, what is the final thought for today, Herman? If you had to summarize the state of zero-click exploits in twenty twenty-six, what would it be?

Herman

I would say that we are in a period of intense transition. The old rules of cybersecurity are being rewritten. We can no longer rely solely on user education. We need more robust, automated defenses that are built into the core of our devices. The age of the invisible attack is here, but so is the age of the invisible defense.

Corn

I like that. The invisible defense. It is a constant battle, but it is one that we are all a part of, whether we realize it or not.

Herman

Precisely. Every time you update your phone, you are participating in that defense. You are making it just a little bit harder for the bad guys to win.

Corn

Well, I think that is a good place to leave it for today. This has been My Weird Prompts. I am Corn.

Herman

And I am Herman Poppleberry.

Corn

Thanks for listening, everyone. We will see you in the next one.

Herman

Stay safe out there, and keep those phones updated!

Corn

You know, it is funny, after talking about this, I kind of want to just go and reboot my phone right now.

Herman

Honestly, me too. I think I will do it as soon as we stop recording. It is just good hygiene.

Corn

It is like washing your hands, but for your digital life.

Herman

Exactly. A little bit of prevention goes a long way.

Corn

I wonder what Daniel is going to send us next. He has been on a real security kick lately.

Herman

Maybe something about biometrics? Or the future of decentralized identity? There is so much happening in that space right now.

Corn

Whatever it is, I am sure it will be interesting. He has a knack for finding the stuff that is just below the surface of the mainstream news.

Herman

That is why we live with him, Corn. He keeps the intellectual environment in the house very lively.

Corn

That he does. Alright, let's head out. I think I hear the kettle whistling in the kitchen anyway.

Herman

Tea and a phone reboot. Sounds like a perfect afternoon.

Corn

Agreed. Thanks again for listening, everyone. We will catch you next time on My Weird Prompts.

Herman

Goodbye for now!

Corn

One last thing, just a reminder that you can find all our past episodes and a lot of other resources on the website. If you want to dive deeper into any of the topics we have discussed, that is the best place to start.

Herman

Right, and the archive is fully searchable, so you can find exactly what you are looking for.

Corn

Perfect. Alright, now we are really going.

Herman

Take care!