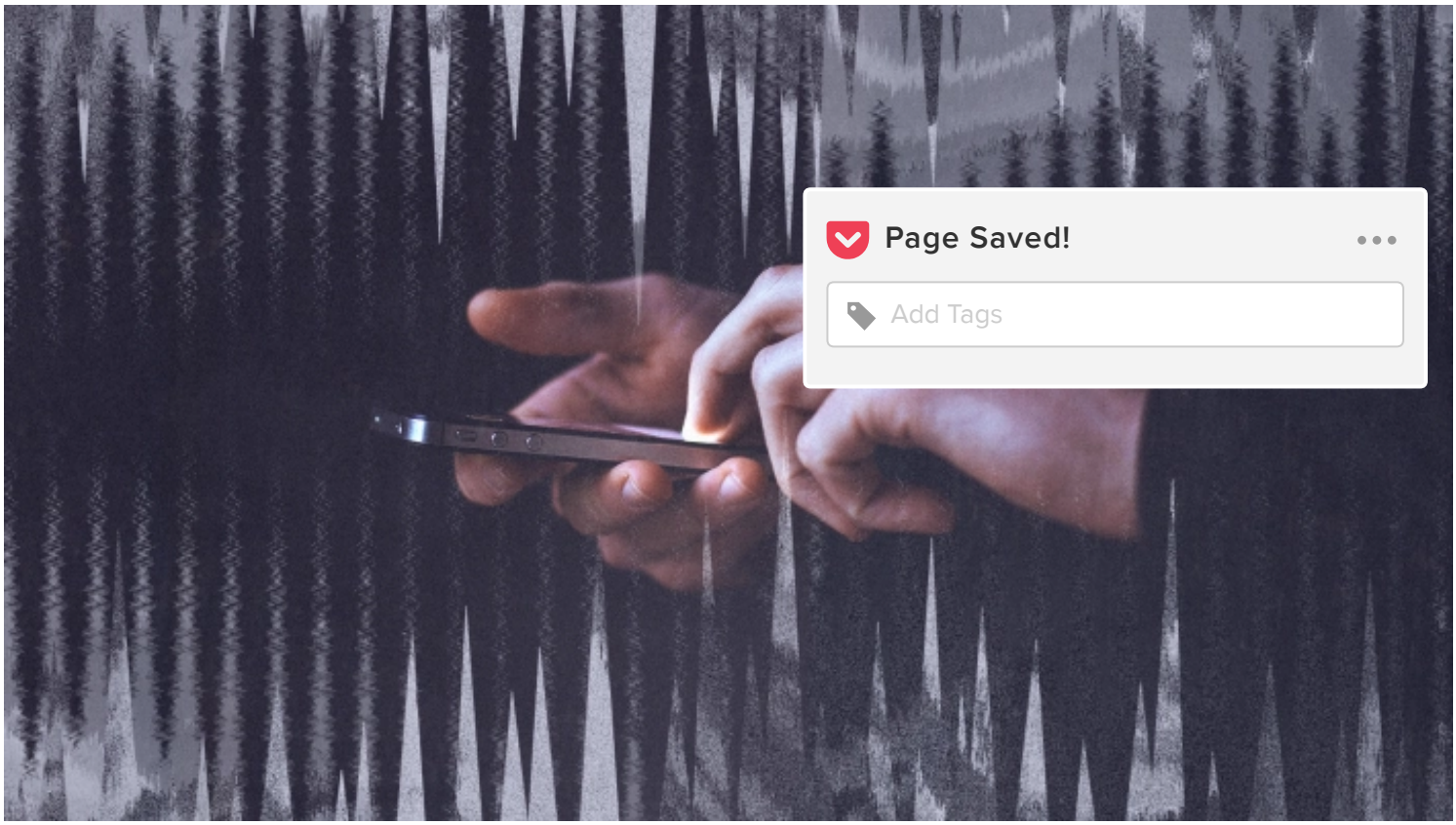
Hackers can take control of the world's most popular voice assistants by whispering to them in frequencies humans can't hear.



[Source Images: Gilles Lambert/Unsplash, photominus/iStock, Marina_Skoropadskaya/iStock]

BY MARK WILSON

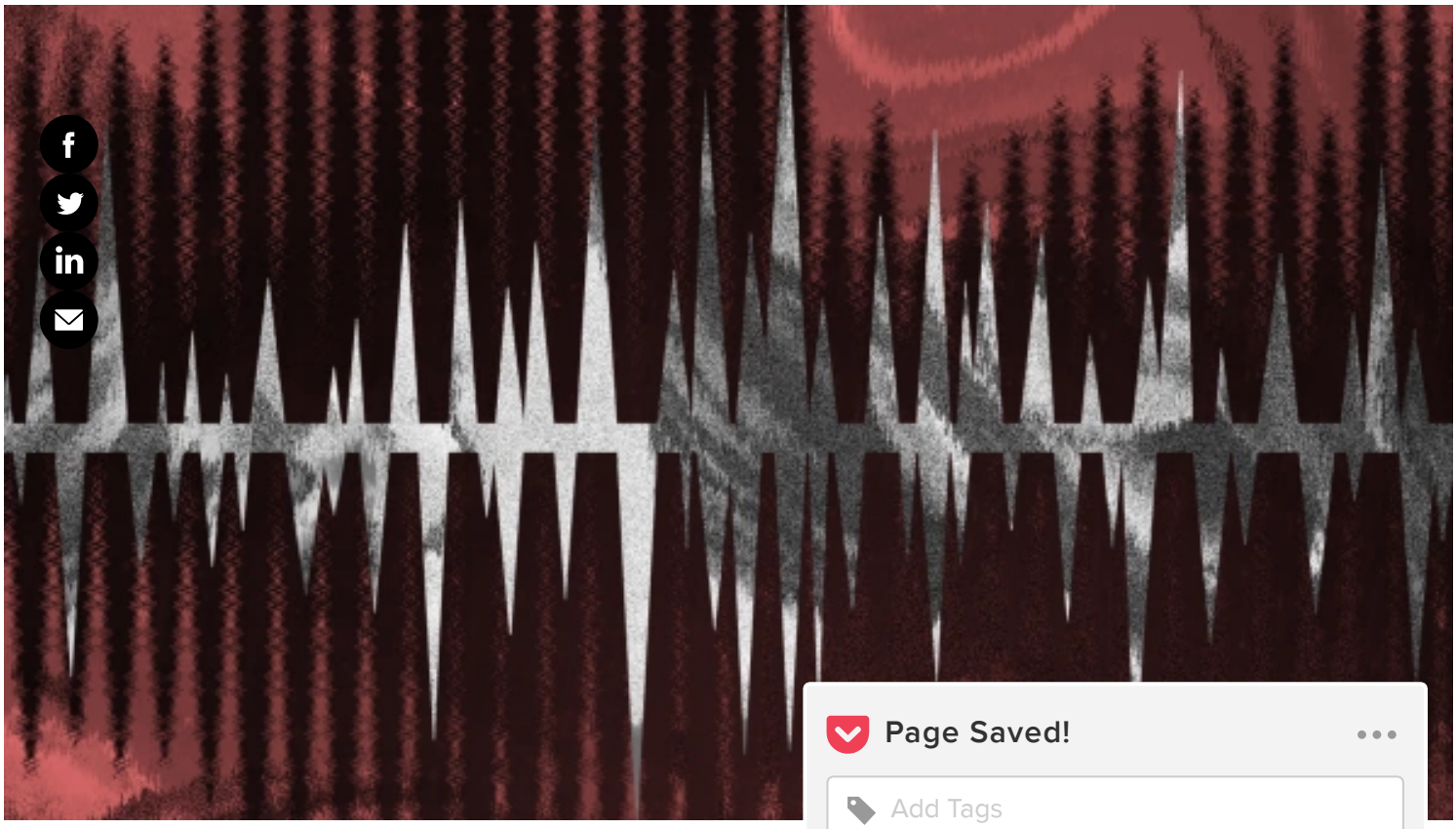
6 MINUTE READ

Chinese researchers have discovered a terrifying vulnerability in voice assistants from Apple, Google, Amazon, Microsoft, Samsung, and Huawei. It affects every iPhone and Macbook running Siri, any Galaxy phone, any PC running Windows 10, and even Amazon's Alexa assistant.

Using a technique called the DolphinAttack, a team from Zhejiang University translated typical vocal commands into ultrasonic frequencies that are too high for the human ear to hear, but perfectly decipherable by the microphones and software powering our always-on voice assistants. This relatively simple translation process lets them take control of gadgets with just a few words uttered in frequencies none of us can hear.

The researchers didn't just activate basic commands like "Hey Siri" or "Okay Google," though. They could also tell an iPhone to "call 1234567890" or tell an iPad to FaceTime the number. They could force a Macbook or a Nexus 7 to open a malicious website. They could order an Amazon Echo to "open the backdoor" (a pin would also be requi
Even an Audi Q3 could have its navigation system redi
commands question the common design assumption th
manipulate a [voice assistant] vocally and can be detec
writes in a paper just accepted to the ACM Conference on Computer and Communications Security.

In other words, Silicon Valley has designed human-friendly UI with a huge security oversight. While *we* might not hear the bad guys talking, our computers clearly can. "From a UX point of view, it feels like a betrayal," says Ame Elliott, design director at the nonprofit SimplySecure. "The premise of how you interact with the device is 'tell it what to do,' so the silent, surreptitious command is shocking."



[Source Images: RamCreativ/iStock, photominus/iStock]

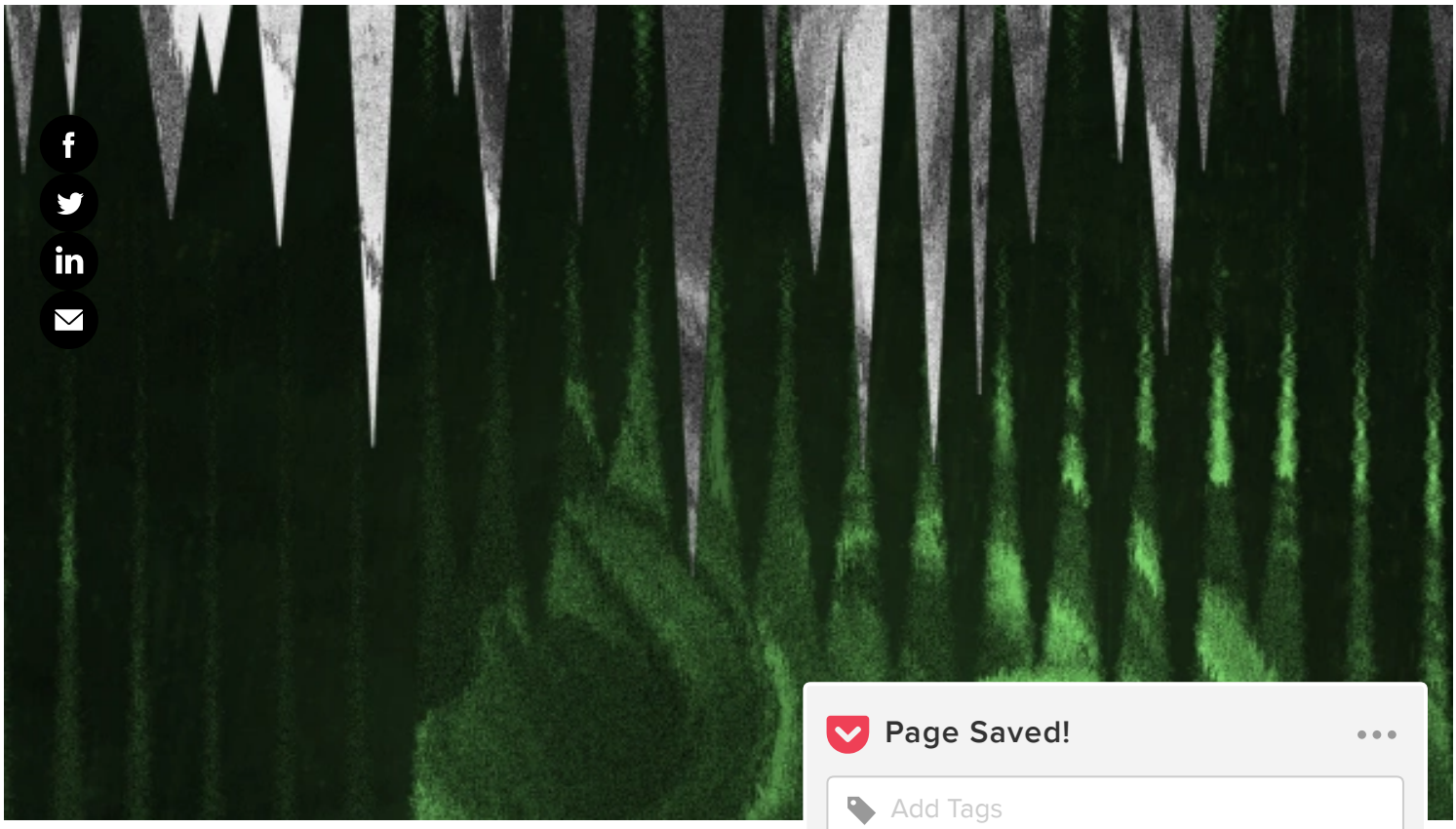
To hack each voice assistant, the researchers used a smartphone with about $3 of additional hardware, including a tiny speaker and amp. In theory, their methods, which are now public, are duplicatable by anyone with a bit of technical know-how and just a few bucks in their pocket.

In some cases, these attacks could only be made from inches away, though gadgets like the Apple Watch were vulnerable from within several feet. In that sense, it's hard to imagine an Amazon Echo being hacked with DolphinAttack. An intruder who wanted to "open the backdoor" would already need to be inside your home, close to your Echo. But hacking an iPhone seems like no problem at all. A hacker would nearly need to walk by you in a crowd. They'd have their phone out, playing a command in frequencies you wouldn't hear, and you'd have your own phone dangling in your hand. So maybe you wouldn't see as Safari or Chrome loaded a site, the site ran code to install malware, and the contents and communications of your phone were open season for them to explore.

The exploit is enabled by a combination of hardware and software problems, the researchers explain in their paper. The microphones and software that power voice assistants like Siri, Alexa, and Google Home can pick up inaudible frequencies–specifically, frequencies above the 20KhZ limits of human ears. (How high is 20kHz? It's just abo
few years ago, which allowed young students who hadn
message friends without their teachers hearing.)

According to Gadi Amit, founder of NewDealDesign and industrial designer of products like the Fitbit, the design of such microphones make them difficult to secure from this type of attack. "Microphones' components themselves vary in type, but most use air pressures that probably cannot be blocked from ultrasounds," Amit explains. Basically, the most popular mics of today transform turbulent air–or sound waves–into electrical waves. Blocking those super-hearing capabilities might be impossible.

That means it's up to software to decipher what's human speech and what's machine speech. In theory, Apple or Google could just command their assistants to never obey orders from someone speaking at 20kHz with a digital audio filter: "Wait, this human is telling me what to do in a vocal range they can't possibly speak! I'm not going to listen to them!" But according to what the Zhejiang researchers found, every major voice assistant company exhibited vulnerability with commands stated above 20kHz.



[Source Images: RamCreativ/iStock, photominus/iStock]

Why would the Amazons and Apples of the world leave such a gaping hole that could, potentially, be so easily plugged by software? We don't know yet, though we've reached out to Apple, Google, Amazon, Microsoft, Samsung, and Huawei for comment. But at least two theories are perfectly plausible, and both come down to making voice assistants more user-friendly.

The first is that voice assistants actually need ultrasonics just to hear people well, compared to analyzing a voice without those high frequencies. "Keep in mind that the voice analyzing software might need every bit of 'hint' in your voice to create its understanding," says Amit of filtering out the highest frequencies in our voice systems. "So there might be a negative effect that lowers the comprehension score of the whole system." Even though people don't need ultrasonics to hear other people, maybe our computers rely upon them as a crutch.

The second is that some companies are already exploiting ultrasonics for their own UX, including phone-to-gadget communication. Most notably, Amazon's Dash Button pairs with the phone at frequencies reported to be around 18kHz, and Google's Chromecast uses ultrasonic pairing, too. To the end user, that imperceptible pairing creates a magical experience that consumers have come to expect in the modern age of electronics ("How's it work? Who cares, it's magic!"). But because we can't hear these mechanisms at work, we also can't tell when they've gone wrong, or when they've been hijacked. They're designed to be invisible. It's the equivalent to driving a car with a silent engine. If the timing belt breaks, you might only realize it when the car inevitably stops and the

odds with security. Our web browsers easily and invisibly
to follow us across the web. Our phones back up our photos
g any focused hacker with a complete repository of our private
e made with easy-to-use technology has come with a hidden
y. This new voice command exploit is just the latest in a growing
gn, but it is, perhaps, the best example of Silicon Valley's
n the face of the new and shiny.

ots in not thinking about how a product may be misused. It's not
ning as it should be," says Elliott. "Voice systems are clearly
se questions . . . It's difficult to understand how the systems
design. I think hard work is needed to undo the seamlessness
ore visibility into how the system works."

For now, there's a relatively easy fix to most DolphinAt
turn off the always-on settings of Siri or the Google Ass
hacker won't be able to talk to your phone (except duri
too). Meanwhile, the Amazon Alexa and Google Home
but is theoretically just as vulnerable) both have hard mute buttons that should do the trick for a majority of the time.

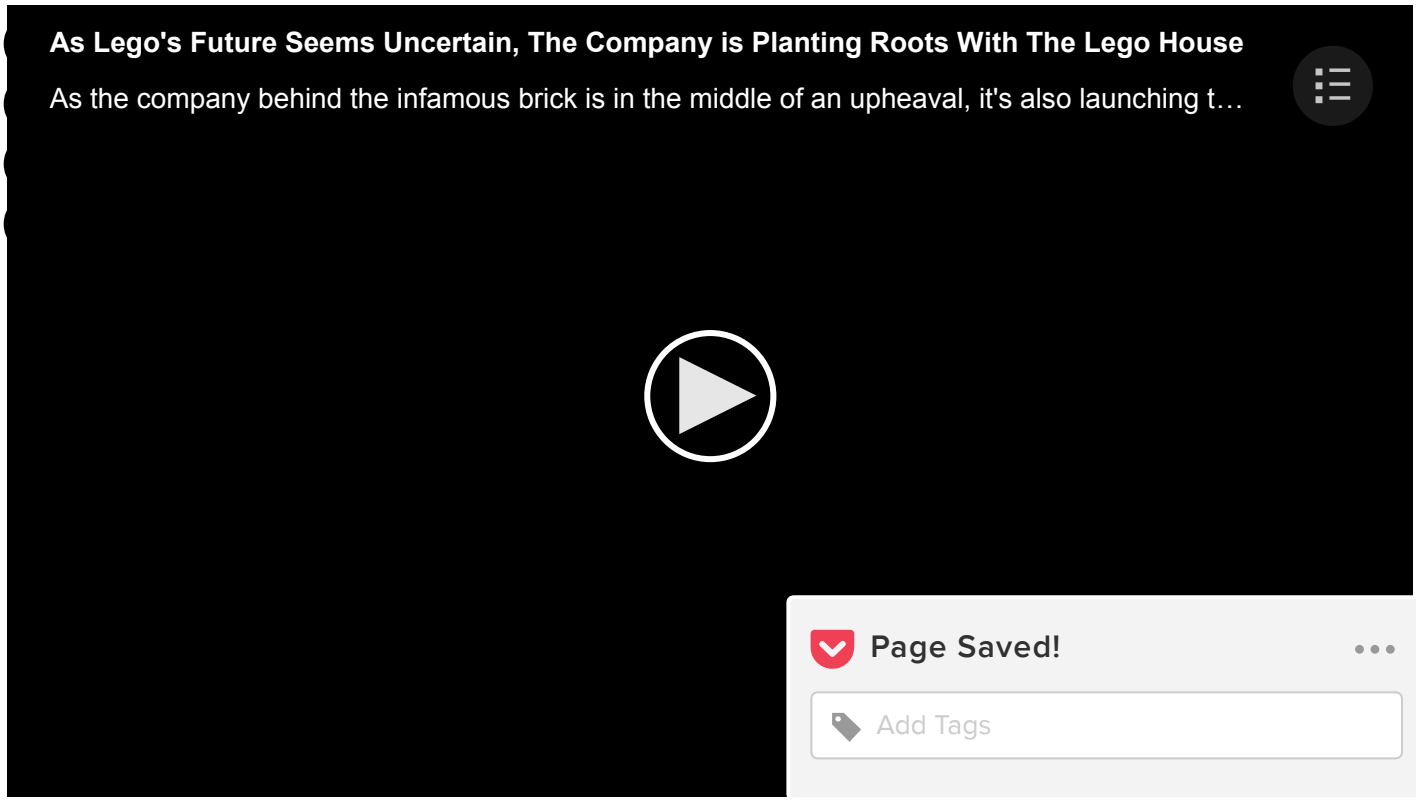
But of course, these solutions are self-defeating. If the only way we can safely use voice assistants is to ensure they're not listening, then what point do they even serve? Maybe these eavesdropping computers don't belong in our lives in the first place–or at least, not anywhere in public.

We've reached out to Apple, Google, Amazon, Microsoft, Samsung, and Huawei and will update this story if we hear back.

ABOUT THE AUTHOR

Mark Wilson is a senior writer at Fast Company. He started Philanthroper.com, a simple way to give back every day. More

VIDEO



As Lego's Future Seems Uncertain, The Company is Planting Roots With The Lego House

As Lego's Future Seems Uncertain, The Company is Planting Roots With The Lego House

How One Design Firm Is Tackling Extremism In The U.K.

This Design Classroom

IDEAS

IDEAS

This Startup Builds Cheap Pop-Up Housing Inside Vacant Buildings

IDEAS

More Or Less Technology In The Classroom? We're Asking The Wrong Question

IDEAS

How Farmers Can Help Ensure That We Don't All Die From Super-Powered Bacteria

ENTERTAINMENT

ENTERTAINMENT

Because Why Not: Ray Liotta Is KFC's Newest Celebrity Colonel Sanders

ENTERTAINMENT

High School Kids Directed Seth Rogen And James Franco In A Hilariously Lo-Fi Short

ENTERTAINMENT

How Microsoft Teamed With A "Wedding Crashers" Producer For A New Creative Ad Model

CO.DESIGN

GRAPHICS

The Glorious Graphic Design Of '70s Porn (NSFW)

PRODUCTS

MIT Invented A New Kind Of Robot Memory

SPACES

How Redesigning Airplane Boarding Could Help Prevent A Pandemic

FAST COMPANY

LEADERSHIP

This Is How To Prepare Your Workforce For A Natural Disaster

NEWS

A Google Drive outage is wreaking havoc right now

IDEAS

This Startup Builds Cheap Pop-Up Housing Inside Vacant Buildings