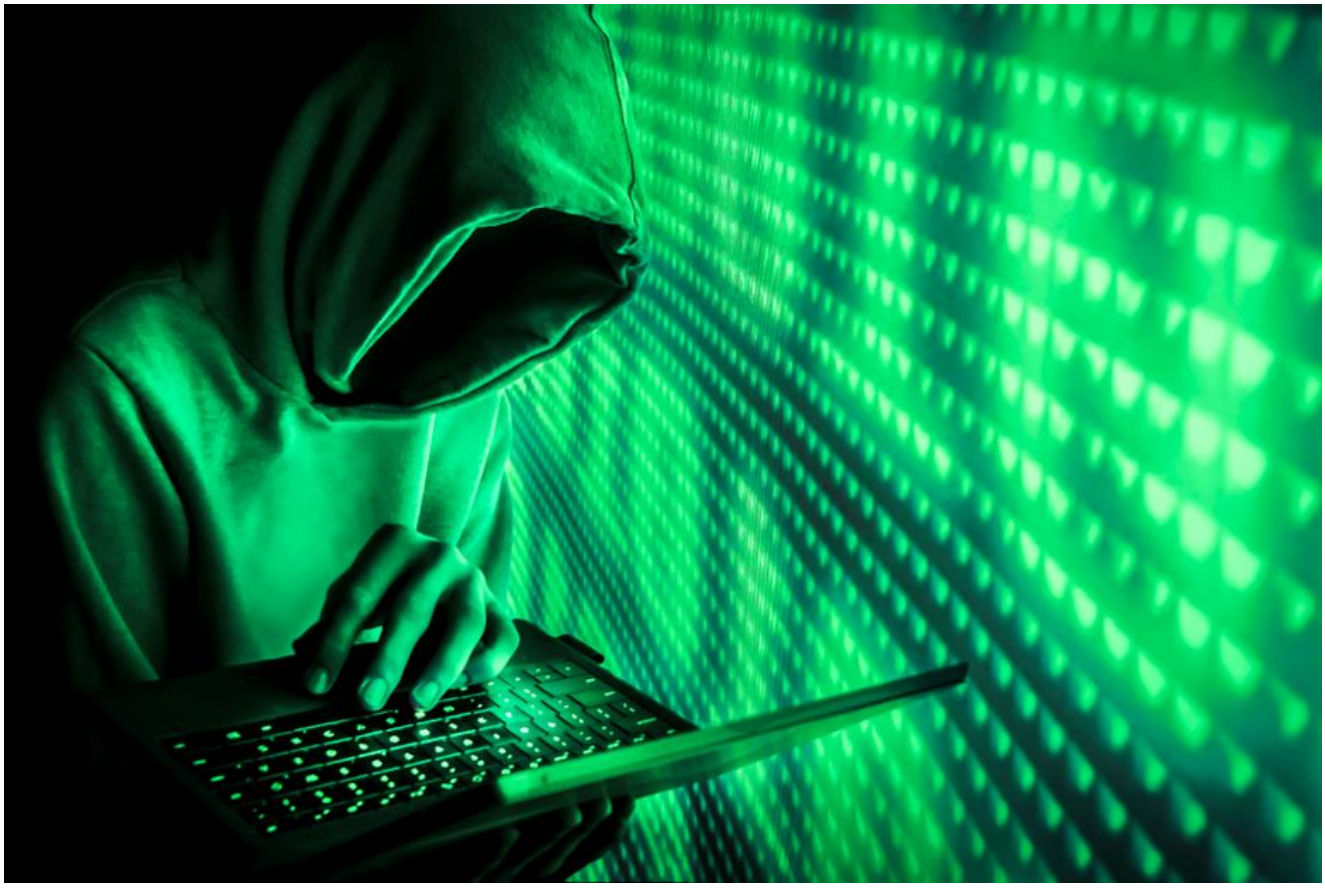
FBI 'Drive-By' Hacking Warning Just Got Real: Here's How This Malicious New Threat Works

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance.



GETTY

"Hackers can use innocent devices to do a virtual drive-by of your digital life," warned the FBI in December. "Unsecured devices can allow hackers a path into your router, giving the bad guy access to everything else on your home network that you thought wa secure." The risk, according to the FBI, was the surge in connected devices at home anc at work. Every one of which is a potential vulnerability.

Well now the reality of that risk has been exposed by the researchers at Check Point, who continue their mission to expose vulnerabilities in the everyday technology we surround ourselves with. The firm's head of research, Yaniv Balmas, tells me that his team decided to target IoT, testing for security holes in these connected smart devices.

And find a serious vulnerability is exactly what they did. "Technically," Balmas tells me "with this exploit I can be 200 or 300 metres away from your home or office. I can take over your device, I can connect to your network." Which makes this the reality of "drive by" hacking. And the devices exposed have been sold by the tens of millions.

Today In: Innovation

According to Balmas, they wanted to emphasise the risks and so selected the simplest and most common endpoint they could think of—smart lightbulbs. "The first company who came up with these smart lightbulbs was Philips Hue," he says. "There's nothing especially smart to say about them—they're lightbulbs that connect to your network. Yo can play with them from your phone, changing colours, it's a cool product."

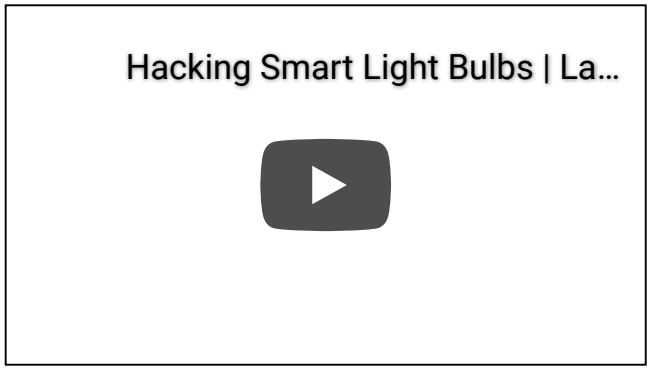
Cool, maybe, but a connected product is a potentially dangerous one. The way in which the bulbs connect is more humdrum than the cool effects you can conjure up from your smartphone. You install a hub in your home and connect it to your network. The bulbs then connect to the hub using Zigbee, the simplest and most common wireless protocol for local IoT connections.

"We wanted to find a vulnerability that enabled us to take over the lightbulb using the Zigbee protocol," Balmas says, and then plays down the trivial risk of "making your house go dark." The team wanted to go further. "We wanted to see if there's an option t infiltrate your network from the lightbulb, to take over that bridge."

If successful, this puts attackers inside your security, opening the risk of planting malware, exfiltrating data, stealing credentials. And it works. The vulnerability was found. And in that instant, tens of millions of smart bulbs had been proven vulnerable. On the surface this flaw is about the way in which Philips Hue implemented Zigbee.

Vulnerabilities with Philips Hue connected lightbulbs have been reported before, the issue here is jumping from the lightbulb to the bridge and from the bridge to the network. In its report, Check Point says it "used the lightbulb as a platform to take over the bulbs' control bridge completely."

In practice, this starts with a takeover of the bulb, knocking it offline and forcing the user to reset it using their control app—this requires it to be deleted and then added back. The compromised lightbulb is then added back, compromising the wider network. This, says Check point, "also enables the hacker to install malware on the bridge—which is in turn connected to the target business or home network."



The protocol "is secure on paper," Balmas says, "the risk is always in the implementation, we found the problem in the Philips implementation. And so Philips can now update the firmware and plug the security gap." This will happen gradually, automatically, and until it's done, the company has an agreement with Check Point not to publish technical details of the flaw with so many millions of devices still at risk.

"We are committed to protecting our users' privacy and do everything to make our products safe," a Philips Hue spokesperson said in a statement. "We are thankful for responsible disclosure and collaboration from Check Point, it has allowed us to develop and deploy the necessary patches to avoid any consumers being put at risk."

Unsurprisingly, this warning isn't really about lightbulbs or Philips Hue, notwithstanding the "huge number" of these devices now open to attack. "Philips is a b European brand," Balmas says. "It takes security very seriously. But there are many others, Chinese or otherwise, that take security much less seriously. If we could find th in Philips think about the implications for all those Chinese devices."

This is the warning. The surge in cheap IoT devices—bulbs, plugs, fridges, rubbish bins toasters—to say nothing of phones, printers, speakers. The cheaper and more "budget" they are, the greater the risk. "We didn't pick those other ones to target," Balmas says, "as it would have been too easy."

In addition to automating firmware updates—or patching manually if there is no automatic option, the FBI recommends fire-walling your core home network from the network on which all these IoT devices connect to you and the outside world. "Your fridge and your laptop should not be on the same network—keep private, sensitive data on a separate system from your other IoT devices."

Balmas agrees. "Update everything. But you also need to understand, that when you connect such a device to your home, you are opening a door to an attacker. The right approach is to segregate these devices. Think 'these devices can be hacked, so I need to separate them.' That's the best approach."

Whatever is connected can be sniffed out. And if there is a known vulnerability for a device seen on the network, that will be used as the entry point—this is how an attacker will work, Check Point says. "As our reliance on IoT becomes an important part of everyday life," the U.S. government warns, "being aware of the associated risks is a key part of keeping your information and devices secure."

There's clearly significant overhead in running separate or gapped networks at home. S until there are consumer devices which automate such security, perhaps the safest rout is taking more care as to the numbers and variety of connected devices we allow into ou home? Just as we should take more care as to the apps we download on our phones, th emails we open, the websites we visit.

Yes, Balmas agrees. That is certainly true.

Follow me on Twitter or LinkedIn.

Zak Doffman

Follow

I am the Founder/CEO of Digital Barriers—developing advanced surveillance solutions for defence, national security and counter-terrorism. I write about the intersectio... **Read More**