Menu Search Bloomberg Businessweek Sign In Subscribe

Cut through the chaos with real time updates on the news affecting the global economy. **Enable Notifications.** Enable Later

December 22, 2021, 5:00 AM EST

The Lock-Picker, the Lockmaker, and the Odyssey to Expose a Major Security Flaw

Dominic Villeneuve figured out a simple way to bypass a widely used door lock, and he told the manufacturer how he did it. A year and a half later, he's telling the world.

Your monthly limit of free content is about to expire. **Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.** Claim This Offer Sign In

Bloomberg Anywhere clients get **free access**

▲ Good Business: The Ethical Hacker

By Adam Bluestein +Follow

Early one morning in June 2020, Dominic Villeneuve woke up and went to his basement workshop to play with a new toy. A friend had given Villeneuve, the director of cybersecurity and infrastructure for a midsize insurance company in Drummondville, Quebec, a lock from a door in a building he was renovating. It was a good one: a Schlage CO-100 commercial-grade, keypad-operated deadbolt, which retails for about $400 and carries a Grade 1 security rating, the highest bestowed jointly by the American National Standards Institute and the Builders Hardware Manufacturers Association.

The locks on most homes are Grade 3, maybe 2. Grade 1 locks are tested to withstand, among other things, 1 million open-close cycles, eight blows starting at 80 joules (comparable to a jackhammer), and five minutes of grinding with a bolt saw. All of the CO-100's electrical and mechanical parts are also certified by the Underwriters Laboratories for resistance to wear and tear, weather, and abuse. But Villeneuve knew he could unlock it without the keypad code. He knew he could beat it.

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.

Claim This Offer

Sign In

Bloomberg Anywhere clients get **free access**

▲ Villeneuve PHOTOGRAPHER: ALEXI HOBBS FOR BLOOMBERG BUSINESSWEEK

In his day job, Villeneuve analyzes and blocks malware attacks on his company's network. Smaller financial-service companies and insurance businesses such as his are a preferred target of hackers, because they often have personal and financial data stored in undersecured networks. His favorite part of the job is playing "red team"—attacking his employer's network with the tricks and gadgets of a better-than-average hacker—to find vulnerabilities. ("Penetration testing" is the technical term.) This also includes looking for ways to covertly access an office or computer and, say, plant a spy pen that has a camera or a USB keylogger to steal logins and passwords. "Every security I see, I try to bypass or find an unexpected way to open it," Villeneuve says. "It's in my DNA."

Villeneuve's father taught him how to assemble and disassemble carburetors when he was 5. Soon, he was taking apart everything in the house. He started picking locks as a teen, practicing on old padlocks and the door of his family home, using

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

photocopied book purporting to be a declassified CIA field manual on lock-picking.

Today he's part of a subculture made up of software types, tinkerers, survivalists, locksmiths, and lawyers and other professionals who enjoy the same three-dimensional puzzles. (He's also co-founder and co-minister of a reform Baptist church in his town.) Members gather for meetups and "sport-picking" competitions that showcase undetectable—"nondestructive," in lock-picking parlance—methods of opening locks for which they don't have keys or codes. "It's better than chess," says Marc Weber Tobias, a lawyer, security consultant, and well-known lock-picker. "It's tactile, it's intellectual, and there are some locks you're just not gonna open."

▲ His kit for competitions and "penetration testing" at work. PHOTOGRAPHER: ALEXI HOBBS FOR BLOOMBERG BUSINESSWEEK

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.

Claim This Offer

Sign In

Bloomberg Anywhere clients get **free access**

with hours of online tutorials? For inquiring minds, the endless corners of YouTube and Amazon.com provide access to information and tools that until recently were generally only available to locksmith guilds, cat burglars, and safecrackers. “In the old manuals on safe manipulation, there’s always a note at the end saying, ‘Now that you’ve read this book, make sure you destroy it,’” says Michael, the principal of e-commerce site Sparrows Lock Picks, who goes by only his first name professionally. “Now everything is posted on YouTube.”

This has helped enthusiasts master the art of the bypass at dazzling speed, accelerating an age-old cat-and-mouse game between lock-pickers and makers as locks are bypassed and videos of triumphs spread online. (The r/lockpicking subreddit, with about 169,000 members, maintains a belt ranking of hundreds of locks; those who crack the hardest ones are black belts.) Pickers are playing red team en masse, exposing weaknesses in products that people trust to keep them safe. It’s forcing manufacturers in what analysts at Verified Market Research call the global physical security industry—a market of at least $125 billion—to live up to their own standards. The relationship between the two camps is uneasy.

One of the most famous names in the community is LockPickingLawyer. In spring 2020, he had about 200,000 subscribers to his YouTube channel, and today he has more than 3.6 million. The retired attorney, who lives in the Washington, D.C., area and asked that his real name not be used, has made almost 1,400 demos, many with hundreds of thousands of views

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

▲ Villeneuve uses specialized picks and “tensioning” tools to bypass a lock. PHOTOGRAPHER: ALEXI HOBBS FOR BLOOMBERG BUSINESSWEEK

Among other thrills, viewers can watch him best a ubiquitous Schlage doorknob lock with a “low skill” attack in about five seconds, open an RFID gun safe with a fork or a spoon, and bypass an allegedly tamper-proof Chinese keypad lock with a Swiss Army knife and a paperclip. LockPickingLawyer’s friend and neighbor, Bosnianbill, who retired from uploading videos in September, had posted more than 1,900 demos since 2007 and has more than 560,000 YouTube subscribers. The Lock Noob, an up-and-comer from the U.K., has over 80,000 subscribers to his channel, which focuses on beginner and intermediate lock-picking. His almost 20-minute *Learn Lock Picking: EVERYTHING You Need to Know!* video has 1 million-plus views.

LockPickingLawyer has no qualms about exposing the illusion

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.

Claim This Offer

Sign In

Bloomberg Anywhere clients get **free access**

hundreds of years is the reason why our security is so bad. There are very few widely used, consumer-grade locks on the market that would even put up an adequate level of resistance to nondestructive entry methods. Consumer education can do nothing but improve that situation."

This isn't a new idea. In 1868, Connecticut locksmith and inventor A.C. Hobbs wrote in *Construction of Locks and Safes* that if a lock was "not so inviolable as it has hitherto been deemed to be, it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance." The question is: How do you spread the knowledge without empowering the dishonest?

The rules of ethical disclosure are complicated. In a deliberately vague example, LockPickingLawyer describes finding a "zero-skill exploit that could be executed by anyone with a small piece of knowledge" on a lock that law enforcement uses widely. He says he

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

he says, leaking his findings to locksmiths groups. “I don’t want to create any dangers or exploits that would be used in the field. However, if a company is not willing to change their product, there’s only so much I can do.”

In most of the U.S., it’s legal to possess lock-picking tools, as long as they’re not used in crimes. On covertinstruments.com, for example, LockPickingLawyer sells a 20-in-1 set called the Covert Companion for $90. Law enforcement tends to apply the “kitchen knife theory,” Michael says. “It’s fine until you point it at someone and start yelling.” Still, sport-pickers and security experts note that few criminals ever bother to pick a lock. According to 2019 FBI Uniform Crime Reporting statistics, about 38% of burglaries involved nonforced “unlawful entry,” and only about 4% of these incidents involved lock-picking. Most home burglaries are sloppy, forced jobs involving screwdrivers, crowbars, and hammers. In commercial burglaries, the latest trend is to smash a stolen vehicle through a wall.

Which isn’t to say that locks don’t matter. When lock-picking is used in a crime, it’s often on a high-value target. The Watergate break-in, for instance, hinged on successfully picking a 4-pound brass lock securing a stairwell. If there’s something valuable to protect, a well-made lock is table stakes. Generally, lock quality goes up with price—and even with the videos available online, or bypasses revealed at annual hacker conventions such as Def Con, discovering quick and easy ways around a Grade 1 lock remains rare. But not impossible.

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.

Claim This Offer

Sign In

Bloomberg Anywhere clients get **free access**

Villeneuve considered the CO-100. He was hoping to add it to the overflowing box of locks he'd defeated.

A humdrum-looking piece of office hardware, the CO-100, introduced in 2011, is a simple, rectangular steel box with a lever handle and a 12-button keypad. It's not connected to the internet, so it can't be reset remotely like a smart lock. It has to be programmed with a three- to six-digit PIN by someone with physical access. The CO-100 typically comes with a traditional keyed lock, too, should the owner need to override the PIN. Allegion, which owns Schlage, touts the lock in marketing materials as durable, affordable, and "versatile enough to use anywhere." And the CO-100 and similar CO-200 models are widely used—in offices, commercial facilities, schools, and multi-unit residential properties. Allegion doesn't break down sales information by product, but these models are perennial bestsellers.

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.

Claim This Offer

Sign In

Bloomberg Anywhere clients get **free access**

Villeneuve could have gone directly at the keyway. But it was more interesting—less tedious—to find a way to manipulate the internal mechanism directly. Removing the CO-100's cover, Villeneuve homed in on a lever beneath the keypad that, when pulled, slid open the deadbolt. Replacing the cover, he considered how to pull the lever from the outside.

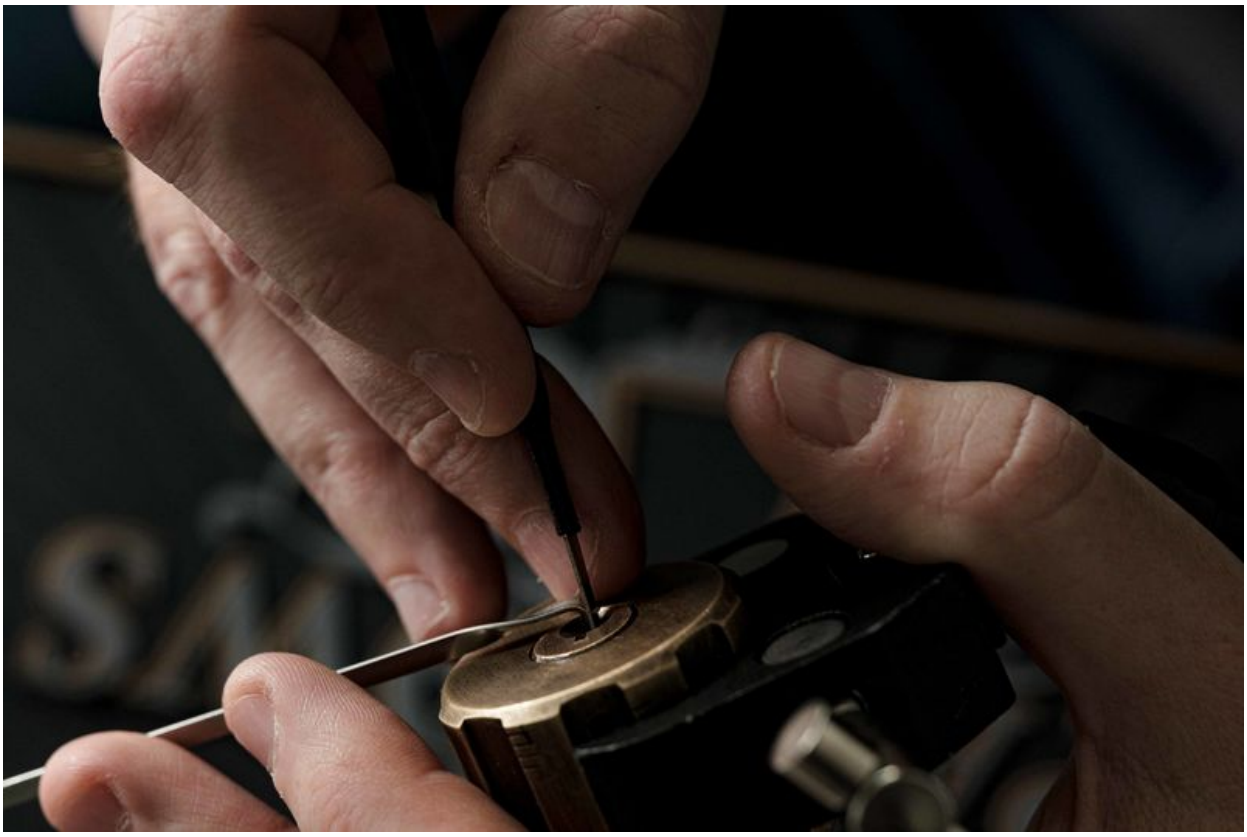
He tried using a magnet to see if it would move a critical spring, but the one he had wasn't strong enough. Then he looked for openings that might let him slide a tool inside. He could get a thin wire through the edge of the keypad but couldn't pull the lever with it. And he didn't like that it left a tiny mark—it was not a truly nondestructive method. Next, he tried a tiny drain hole at the bottom of the lock housing, there to let moisture escape. When the lock is attached to a door, the hole is almost unnoticeable. Villeneuve started probing it, first with thin strips of metal, and then with various-size zip ties, until he found a fit. Then he cut a notch into one end of the zip tie to hook the lever.

At about 6 a.m., two hours after he started working on the lock, he pushed his homemade tool through the drain hole, caught the lever, gave a gentle tug, and the lock sprung open. When he reinserted the zip tie and pulled again, it locked. It worked again, and again, and again. Bursting with energy, Villeneuve worked out in his home gym and showered. He could barely contain his enthusiasm at breakfast when he revealed yet another hack to his wife. He says she was unfazed. "Cool, it sounds easy," she responded.

At his office that day, Villeneuve walked down a hallway

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

to execute a bypass under controlled conditions, another to do it in the wild. And another altogether to do it with a tool that costs basically nothing and was everywhere he looked, since zip ties are used to wrangle computer cords. “I’ve found many vulnerabilities in my life,” Villeneuve says. “But this one is so easy, and so dangerous, that it’s different from the others. Even if an alarm goes off, police will find no trace of an infraction.”



▲ Villeneuve picking a lock that has been removed from a door. PHOTOGRAPHER: ALEXI HOBBS FOR BLOOMBERG BUSINESSWEEK

A search on the internet and dark web convinced him that he’d found something new, and as a self-proclaimed “ethical” lock-picker, he reached out to Schlage. Founded in San Francisco in 1920 by German immigrant Water Schlage, the company had some important early patents; five years later, it was making 20,000 locks a month. When Ingersoll Rand Inc. acquired the company in

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

In 2013, Schlage and the rest of Ingersoll Rand's security technology business was bought by Allegion. Headquartered in Dublin, the company has 30 global security brands. It took in $2.7 billion in revenue in 2020, and its stock price has climbed from about $80 in early 2019 to about $125 today. In North America, Allegion is the No. 1 maker of products that control how people enter and exit buildings—locks and locksets, doors and door frames, hinged door closers, push bars, electronic access systems, and more. Unlike software manufacturers, who make it easy for hackers to report bugs, most lockmakers don't have a formal channel to receive tips about vulnerabilities. Villeneuve says it took him a few days to find someone to take down the details of his discovery.

On June 27, 2020, he sent an email with the subject line "Major vulnerability in CO-100 (maybe CO-200)" to Allegion's head of public relations. He attached two videos demonstrating his bypass. "I want to be honest and give you the opportunity to offer a fix to your clients before someone found it and make it public on Internet," wrote Villeneuve, whose first language is French.

Two days after he sent his email, he was put in touch with Allegion's global director of cybersecurity, Frank Kasper. In emails, calls, and video chats, Villeneuve explained the bypass. He taught Allegion engineers how to duplicate it and brainstormed fixes. On July 10, Kasper wrote that engineers were working on a snap-in part to plug the drain hole that wouldn't require removing locks from doors. At the end of August, he sent Villeneuve a prototype. Three days later, Villeneuve wrote back to say he'd removed the

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

In early December, Kasper wrote Villeneuve with good news. His engineering team had redesigned the CO-100 and related products to address the drain hole problem. But Kasper wrote that delivery was delayed because of supply chain issues—"parts are in transit from our supplier in China to our manufacturing facility in Mexico." On Feb. 25, 2021, Kasper shipped Villeneuve the redesigned lock and another version of the snap-in retrofit part. Villeneuve was pleased with both. Although he still managed to pick the keyed component, it was a challenge, he wrote Kasper, adding, "I cannot imagine picking it in the field." The new retrofit plug, he said, was "a very good fix" that he couldn't bypass in a nondestructive manner. "Frank is a very great guy," Villeneuve says.

Their interaction reflects an evolving model in the industry, which is inching toward the détente software makers have with so-called white hat hackers. In that system, monetary "bug bounties" encourage hackers to report weak code; good bug catchers spin their skills into consulting work. "Fifteen years ago, we were the most hated guys in the industry," says Tobias, the lawyer and security expert, who has a string of legendary bypasses. "Now they realize we're their best asset. Lock-pickers see things in a different way than engineers at lock companies. They care about how to make things work. We look at how they can break."

For a decade at Def Con, the annual hacker convention in Las Vegas, Tobias owned Big Lock in an embarrassing string of demonstrations. In 2007 he bested Medeco's high-security M3 with a "bump key," or custom blank, and a paperclip. In 2013 he beat

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

consulted for most of them, including Swedish conglomerate Assa Abloy AB (owner of Medeco, Arrow, Mul-T-Lock, and Yale) and Allegion (which also owns Steelcraft, a maker of doors and door frames, and Kryptonite, which produces bike locks).

In an October email to *Bloomberg Businessweek*, Allegion said it evaluates the security of its products in many ways, including "extensive third-party assessments" and "external reports of potential vulnerabilities." But, Tobias says, "you're going to get sued if someone is raped, robbed, or killed because of a problem you knew about." All it takes is one person on YouTube to expose the known flaw.

In March, Kasper and Villeneuve discussed a consulting arrangement. Villeneuve would test new Allegion locks and confidentially report vulnerabilities. He didn't want money in return; he just wanted a shot at the hardest puzzles that one of the world's top lockmakers could throw at him. But in mid-July, Kasper wrote that managers had nixed the idea. Still, he said he wanted to send Villeneuve the occasional product to "hack" in the future.

It was now more than a year since he'd reported the issue with the CO-100. The redesigned lock and retrofit part had been ready since February. Where, Villeneuve wondered, was the public notification? When were customers going to know?

He expressed his frustration to Kasper, though he says he "never made an ultimatum. I just wanted them to do the right thing." On July 16, 2021, Kasper wrote that he'd talked with upper

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

time. The lawyer assured him there were “actions under way to notify customers about the fix,” according to video of the call. The next day, Villeneuve wrote Kasper to decline the gig, citing the complications of working for a U.S. company in Canada. (Schlage is now headquartered in Carmel, Ind.) But he said that he was “glad to hear you say that you are ready to make a fix available.”

In August, with no news from Allegion about notifying the public, Villeneuve considered announcing the vulnerability himself. But he decided against it, because he wanted customers to have access to the retrofit first. Tobias says he’s seen people demand that lockmakers pay ransoms up to $50,000 to keep a vulnerability under wraps. But for ethical lock-pickers, it’s about the recognition. “If you stand against a big company to make it fix something, that marks you as an ethical lock-picker,” Villeneuve says. “When you give a talk at a security conference and people Google you, they see what you did, and that gives you a lot of credibility.” But it’s important to be first. The bypass Villeneuve discovered was so obvious, it was only a matter of time before another person figured it out, too, and posted a video to timestamp the discovery.

In the October email to *Businessweek*, an Allegion spokesperson confirmed but downplayed the issue: “Importantly, the mechanical vulnerability is not due to normal operations or daily use of the lock, but occurs when a unit is intentionally manipulated in an unusual way.” The spokesperson added that “replicating the vulnerability requires a customized tool and an individual who understands the mechanics of the lock—so it’s not

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

Villeneuve says that's laughable: "I'm proud that I've mastered the manipulation of a zip tie. The fact that a bunch of their engineers were not able to find how I did this does not mean that the bypass is hard to do, just that they don't have a hacker's mindset."

The spokesperson wrote that Allegion emailed a bulletin titled "Schlage CO Series Mechanical Security Enhancement" in July. It went to "customers and distributors who have potentially vulnerable units" purchased before February 2021, including the CO-100, CO-200, CO-220, and CO-250. The alert urged all lock owners to install the retrofit part, which the company would send out free—but only upon request.

It's not clear who saw the bulletin. Contacted this fall, eight locksmiths and distributors from across the U.S. who sell Schlage products said they were unaware of a problem. "In fact, in the past few months, we've seen an increase in CO-100 locks" sold, wrote Patrick Duff, director of multifamily and hospitality industry sales at GoKeyless in Miamisburg, Ohio, which installs as many as 15,000 locks a year nationwide.

Villeneuve says that no one from Allegion mentioned the bulletin to him and that the insurer he works for wasn't notified. There's no trace of it online. Allegion emailed the bulletin to *Businessweek*; after reviewing it, Villeneuve noticed one photo included was a still from a video he'd sent the company.

The spokesperson declined to disclose how many people got the bulletin, or how many retrofit parts have been shipped, saying "it could negatively impact the safety of our customers." The

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

and Allegion wouldn't provide a link to. The spokesperson adds: "These customers can ultimately help to remediate issues for commercial-market products. The portal is not intended, or even relevant, for the general public." (In December another spokesperson said "we've received numerous requests for the simple, no-charge solution offered in the bulletin; so we are confident ... customers and distributors have received the information.")

Villeneuve is vehement: The onus is on the company, not customers, to spread the word. "I understand they don't have a way to reach their millions of clients personally, but why don't they just send a bunch of fixes to every distributor, and after two weeks, make a public announcement?" he asks. "When there is a recall for a cell battery getting on fire with no reason, they do some public announcement and provide a free replacement battery at local shops. In this case, they have a cheap fix for an easy-to-do hack, and no one knows about it."

Regardless of how wide a release the Allegion bulletin got, that the subject line flags an "enhancement," not a major security issue, is potentially confusing. "At the very least, it would make me ask myself, 'Why did they do this?' And more importantly, 'What happens if I don't do this?'" says Duff, of GoKeyless. Without a broad public alert or recall, Villeneuve says, consumers can't know if they're buying the improved lock or the old one because there's no indication on the label.

Historically, lock manufacturers have issued public alerts only after they've been sued or someone comes forward to expose a

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

Ingersoll-Rand an estimated $10 million in replacement costs. In 2011, Kaba (now Dormakaba Holding AG) was sued over a vulnerability in its push-button Simplex locks, which the company knew could be hacked with a rare earth magnet; the lock was redesigned, and a free retrofit issued. Both companies acted only after people exposed problems that were already well known to security insiders.

What, if any, damage has been done at this point is hard to say. That's the nature of a nondestructive bypass. Who knows if Villeneuve is the first person to discover the zip-tie trick? Others may have used it, or a similar one, to gain covert access to offices and properties for years. He's designed a stainless steel version of the drain hole plug that's available for a few dollars on the Sparrows Lock Picks site, but that's not a substitute for the company taking action.

Finally, on Dec. 10, Villeneuve decided it was time to go public: Allegion's retrofit part was available, as was his. He released an almost five-minute-long video documenting the discovery on his DHack Security YouTube channel, and within five days it had 3,100 views. Lock Noob posted a reaction video to Villeneuve's, which itself got almost 4,000 views in that span. "It's not something I would ever have figured out on my own," Lock Noob says in his video.

Allegion says the number of affected locks on the market is "significantly lower" than the "millions" of units Villeneuve claims in his video. The company issued a formal reaction in a Dec. 20 email: "Allegion appreciates the beneficial role of external

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.
Claim This Offer
Sign In
Bloomberg Anywhere clients get **free access**

products and work to benefit end users and public safety. We saw a potential vulnerability, addressed it, and communicated to channel partners and distributors. We feel the best route is to let manufacturers inform customers rather than sensationalize it."

For Villeneuve, going public was less about sensationalizing anything than making sure the locks get fixed. "It's OK to find a vulnerability, to make it public, to make some reputation," he says. "But if showing the way I handled it motivates people to communicate with manufacturers, that's the goal. To make things more secure."

Read next: How Thieves Stole $40 Million of Copper by Spray-Painting Rocks in Turkey

---

Terms of Service Do Not Sell My Info (California) Trademarks Privacy Policy
©2021 Bloomberg L.P. All Rights Reserved
Careers Made in NYC Advertise Ad Choices Help

Your monthly limit of free content is about to expire.
Stay on top of historic market volatility. Try 3 months for ~~$8.75~~ $0.50 per week. Cancel anytime.

Claim This Offer

Sign In

Bloomberg Anywhere clients get **free access**