RISK ASSESSMENT / SECURITY & HACKTIVISM

Internet of Things security is so bad, there's a search engine for sleeping kids

Shodan search engine is only the latest reminder of why we need to fix IoT security.

by J.M. Porup (UK) - Jan 23, 2016 10:30am EST

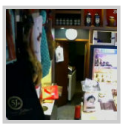
Shodan, a search engine for the Internet of Things (IoT), recently launched a new section that lets users easily browse vulnerable webcams.

The feed includes images of marijuana plantations, back rooms of banks, children, kitchens, living rooms, garages, front gardens, back gardens, ski slopes, swimming pools, colleges and schools, laboratories, and cash register cameras in retail stores, according to Dan Tentler, a security researcher who has spent several years investigating webcam security.

"It's all over the place," he told Ars Technica UK. "Practically everything you can think of."

We did a quick search and turned up some alarming results:

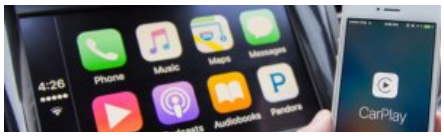
A sleeping baby in Canada

The cameras are vulnerable because they use the Real Time Streaming Protocol (RTSP, port 554) to share video but have no password authentication in place. The image feed is available to paid Shodan members at images.shodan.io. Free Shodan accounts can also search using the filter port:554 has_screenshot:true.

Shodan crawls the Internet at random looking for IP addresses with open ports. If an open port lacks authentication and streams a video feed, the new script takes a snap and moves on.

LATEST FEATURE STORY



One week with Apple's CarPlay

Pretend your awful stock car system doesn't exist with Apple's casted interface.

WATCH ARS VIDEO

CES 2016: Ars walks the length and breadth of CES so you don't have to

Ars Technica Automotive Editor Jonathan M. Gitlin walked the length and breadth of the Consumer Technology Association conference (CES) in Las Vegas, Nevada.

STAY IN THE KNOW WITH

LATEST NEWS

Mission: Red Planet brings steampunk Martian domination to your tabletop

Cute to "a little sinister"—the beauty of US spy satellite rocket launch logos

GET TO THE ÜBER!!!

At the Sundance Film Festival? You can try Airbus and Uber's new helicopter ride

BOOSTER BATTLES

While the privacy implications here are obvious, Shodan's new image feed also highlights the pathetic state of IoT security, and raises questions about what we are going to do to fix the problem.

Of course insecure webcams are not exactly a new thing. The last several years have seen report after report after report hammer home the point. In 2013, the FTC sanctioned webcam manufacturer TRENDnet for exposing "the private lives of hundreds of consumers to public viewing on the Internet." Tentler told Ars he estimates there are now *millions* of such insecure webcams connected and easily discoverable with Shodan. That number will only continue to grow.

So why are things getting worse and not better?

The curse of the minimum viable product

Tentler told Ars that webcam manufacturers are in a race to bottom. Consumers do not perceive value in security and privacy. As a rule, many have not shown a willingness to pay for such things. As a result, webcam manufacturers slash costs to maximize their profit, often on narrow margins. Many webcams now sell for as little as £15 or $20.

"The consumers are saying 'we're not supposed to know anything about this stuff [cybersecurity]," he said. "The vendors don't want to lift a finger to help users because it costs them money."

If consumers were making an informed decision and that informed decision affected no one but themselves, perhaps we could let the matter rest. But neither of those conditions are true. Most consumers fail to appreciate the consequences of purchasing insecure IoT devices. Worse, such a quantity of insecure devices makes the Internet less secure for everyone. What botnet will use vulnerable webcams to launch DDoS attacks? What malware will use insecure webcams to infect smart homes? When 2008-era malware like Conficker.B affects police body cams in 2015, it threatens not just the reliability of recorded police activity but also serves as a transmission vector to attack other devices.

FURTHER READING

POLICE BODY CAMS FOUND PRE-INSTALLED WITH NOTORIOUS CONFICKER WORM

One of the world's most prolific pieces of malware is found in cams from Martel.

"The bigger picture here is not just personal privacy, but the security of IoT devices," security researcher Scott Erven told Ars Technica UK. "As we expand that connectivity, when we get into systems that affect public safety and human life—medical devices, the automotive space, critical infrastructure—the consequences of failure are higher than something as shocking as a Shodan webcam peering into the baby's crib."

Admiring the problem is easy. Finding solutions is harder. For his part, Tentler is sceptical that raising consumer awareness will be enough to solve the problem. Despite tons of press harping on about the privacy implications of webcams, it's pretty clear, according to Tentler, that just telling people to care more about security isn't going to make a difference.

Instead, he argues it's time to start arm-twisting vendors to release more secure products.

FTC to the rescue?

When it comes to strong-arming manufacturers, government entities like the US Federal Trade Commission (FTC) may be able to help. Ars UK spoke with Maneesha Mithal, associate director of the FTC's division of privacy and identity protection, and she was quick to mention several examples where the organization went after at-fault companies. In recent years according to Mithal, the FTC has prosecuted more than 50 cases against companies that did not reasonably secure their networks, products, or services.

The FTC takes action against companies engaged in deceptive or unfair business practices, she explained. That includes IoT manufacturers who fail to take reasonable measures to secure their devices.

"The message from our enforcement actions is that companies can't rush to get their products to market at the expense of security," she said. "If you don't have reasonable security then that could be a violation of the FTC Act."

In addition to the precedent-setting enforcement action against TRENDnet, the FTC also issued security best practices for IoT manufacturers back in January 2015, urging them to bake in security at the design phase rather than bolting it on as an afterthought. Vendors should train their employees in security best practices, the FTC said. Such practices could be a "defence-in-depth" strategy to mitigate risks, pushing security patches to connected devices for the duration of the product life cycle, and so forth.

Blue Origin soars again, successfully reusing its New Shepard rocket

Models of pedestrian flow stumble because people change their minds

How the smartphone changed everything, or, the rise of BYOD in the workplace

This is all sensible, top-notch security advice. The FTC even followed up with an official guidance document in June and a series of workshops for businesses on improving their security posture.

Erven told us that these new guidance documents are a warning to businesses to improve—or else. "The thing that really does come next after guidance is regulation, if they don't pick up their game and implement [the official security guidance]."

It may already be too late to avoid regulation. Mithal told Ars that the FTC has asked Congress for federal data security legislation that would give the commission the authority to seek civil penalties for companies that don't implement reasonable security. Rather than mandate highly prescriptive, technology-specific legislation (for instance, "you must use this firewall and that kind of encryption"), the FTC seeks a process-based approach that will remain valid even as technology continues to advance.

A *Which?* for IoT security

Many people we spoke to for this story were leery of too much regulation since it could discourage further innovation in the IoT space. But as an alternative, could a *Which?* (UK) or *Consumer Reports* (US)-style rating system help IoT manufacturers solve the problem without regulation?

One such solution would be for a trusted industry or government body to rate the security of devices. This would help consumers make an informed decision about what products to buy in the same way that Euro NCAP or the US National Highway Transportation Safety Administration (NHTSA) uses a five-star safety rating for cars. You don't have to be an car engineer to make sense of a car safety rating. Why should you have to be a computer security expert to make sense of IoT security?

"The solution has to be driven by customer awareness to security," Erven argued. "In order for an informed consumer to make a decision, they have to have an understanding of the security posture among devices."

I Am The Cavalry, a group of concerned security researchers focused on critical infrastructure, is working on a five-star rating system for consumer IoT. The rating system will give consumers the "quick ability to check device security without having to understand the technical details."

Security researcher Brian Knopf is leading I Am The Cavalry's charge for a simple security and privacy rating system for IoT devices, which he hopes to release early in 2016. He shared with Ars some of the preliminary criteria that IATC will use to judge devices:

Security

1. Secure by Default
    1. No default passwords shared between devices, or weak out of the box passwords.
    2. All passwords should be randomly created using high quality random number generators.
    3. Advanced features used by small percentage of users should be turned off (VPN, Remote Administration, etc.).

2. Secure by Design
    1. Firmware should be locked down so serial access is not available.
    2. Secure Element (SE) or Trusted Protection Modules (TPM) devices should be used to protect access to the firmware and hardware.
    3. All GPIO, UART, and JTAG interfaces on the hardware should be disabled for production versions.
    4. NAND or other memory/storage mediums should be protected with epoxy, ball sockets (so the memory cannot be removed and dumped), or other methods to prevent physical attacks.

3. Self-contained security
    1. The devices should not rely on the network to provide security. Rather, the device's security model should assume the network is compromised and still maintain

protection methods. This can be done with prompts to the users to accept handshakes between devices trying to access other devices on their networks.
2. Communication between devices should be encrypted to prevent MitM attacks and sniffing/snooping.

Privacy

1. Consumer PII not shared with manufacturers or partners
2. Usage data on individual consumer is never shared with partners or advertisers.
3. Anonymous data for buckets of users on usage patterns is acceptable as long as it's proven to not be traceable back to the individual consumers.
4. Data collection policy, type of data collected and usage of data is clearly documented on site.

Vendors will be invited to submit their pre-production devices for testing, Knopf said, along with the star rating they are applying for. Researchers will then test the devices to ensure they meet the manufacturer's claims.

"The vendor would then receive a preliminary test report that they could respond to, either to fix items before production or accept the rating," he explained. "The final report would then be posted online for any consumer to review, or security tester to validate."

Knopf said the program would not depend on the willing participation of manufacturers. Independent researchers would also be welcome to test off-the-shelf IoT devices against the criteria and post the results on the I Am The Cavalry website. This, he hopes, will encourage manufacturers to improve their products.

Enter the Pentagon

The US Air Force is funding a similar, unrelated initiative. Peiter "Mudge" Zatko is a member of the high-profile L0pht hacker group who testified before Congress in 1998, and since he's gone on to head cybersecurity research at the Defense Advanced Research Projects Agency (DARPA) before joining Google in 2013. In June, Zatko announced he was leaving the search giant to form a cybersecurity NGO modelled on Underwriters Laboratories.

The new initiative, Cyber Independent Testing Laboratory (CITL), won a $499,935 (£350,000) contract from the US Air Force in September to create a "Consumer Security Reports," according to a report by Inside Cybersecurity. Mudge declined to comment for this article, instead referring us to the interview with Inside Cybersecurity:

> "Our intention is to provide [consumers] with the information and tools they need, in a non-partisan fashion, and without profit incentives getting in the way of providing unbiased and quantified ratings of the software and systems they are purchasing," Zatko said. "Think of this as a cybersecurity parallel to nutritional facts on food, energy star ratings on appliances, or vehicle information guides in the windows of new cars."
>
> [...]
>
> "The IoT is a part of this environment," he continued. "We will include analysis and comparative ratings, on the robustness and security in software, for IoT devices as well as more traditional operating systems, applications and services."

Mudge told Ars that "The procedures and methodologies will be made public in 2016. It includes firmware for IoT."

Last week in an interview with the Council on Foreign Relations (CFR) blog, he identified four goals for CITL:

> Consumers having the ability to comparatively distinguish safe products from unsafe, secure from insecure;
>
> Pressure on developers to harden their products and engage in defensive development practices;
>
> The ability to quantify risk; and
>
> Take away low-hanging fruit, such as the more insecure product development practices, and

thus begin to devalue parts of the exploit market.

Mithal said the FTC was aware of the efforts by both I Am The Cavalry and CITL, and the group welcomed initiatives that educate consumers about security. “My concern,” she said, “would be that companies should bake in security whether consumers shop on that basis or not. The onus shouldn’t be on the consumer to figure this out.”

But will these efforts stop attackers?

Some combination of regulatory stick and rating system carrot seems likely to increase IoT security across the board. The Internet is a minefield of accidents and adversaries, and reducing opportunistic malware infection, like preventing Conficker.B infection of police body cams, is low-hanging fruit.

But unlike the electrical appliances Underwriters Laboratories has traditionally tested for safety, or even Euro NCAP's safety ratings that have encouraged car makers to manufacture safer vehicles, both regulation and cybersecurity product ratings seem powerless to stop determined attackers.

When Mudge announced his plan to form CITL back in June, security researcher Rob Graham went so far as to call the plan a “dumb idea”:

> **It’s not the same quality problem**
>
> UL is about accidental failures in electronics. CyberUL would be about intentional attacks against software. These are unrelated issues. Stopping accidental failures is a solved problem in many fields. Stopping attacks is something nobody has solved in any field.
>
> In other words, the UL model of accidents is totally unrelated to the cyber problem of attacks.

Graham affirmed his critique in a Twitter direct message to Ars. “UL doesn’t test systems for somebody deliberately trying to attack them,” he wrote. He also argued that CITL “adds a lot of bureaucracy for little value.”

Mitigating risk is not the same as eliminating it. But until someone figures out to deal with deliberate attacks, the problem of insecure IoT devices looks set to get worse before it gets better.

Erven said it best: “Our dependence on technology is growing faster than our ability to secure it.”

So buckle up, kids, we’re in for a bumpy IoT ride over the next few years. And while you're at it, put a password on that webcam in your kid's bedroom. No one wants to unexpectedly show up in search results.

J.M. Porup is a freelance cybersecurity reporter who lives in Toronto. When he dies his epitaph will simply read "assume breach." You can find him on Twitter at @toholdaquill.

This post originated on Ars Technica UK

READER COMMENTS 66

1572 169 99

← OLDER STORY | NEWER STORY →

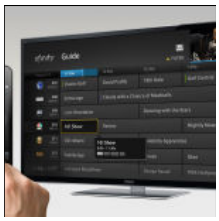
YOU MAY ALSO LIKE

AMD slams “biased” and “unreliable” Intel benchmarks

Yet another bill seeks to weaken encryption-by-default on smartphones

Media devices sold to feds have hidden backdoor with sniffing functions

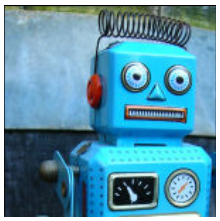
9 baby monitors wide open to hacks that expose users’ most private moments



CableCard could finally get a card-less replacement

Ars UNITE: Join us to talk about the future of the Internet of Things

Oracle settles with FTC over Java's "deceptive" security patching



Fight the future: Ars readers say "NO" to the Internet of Things