IOT THREAT LANDSCAPE

Old hacks, new devices

F-Secure

ALEXA, ARE YOU LISTENING?

In early 2017, security researcher Mark Barnes discovered a way to turn 2016 models of Amazon's Echo into an "expensive microphone."[1]

If an attacker had physical access to the device it was possible to install malware into the home personal assistant without leaving a trace. Once that happened, the device could be monitored from anywhere in the world.

Though researchers had speculated that it might be possible to install software on the Echo through debug pads at the base of the device, this was the first successful example of an attacker gaining remote access to Amazon's smart speaker system. It was also a glaring preview of the sort of worst-case scenarios consumers could face when connecting their appliances to the internet.

Who would buy a smart home device if it could be turned into a "wiretap?"

Yes, you'd probably have to have a serious hacker in your inner circle for your Echo to have been vulnerable to this attack. But the two design choices that made this vulnerability possible provided another tool in the arsenal of motivated attackers who prey on high value targets as they travel to hotel rooms around the world.

Mark and his colleagues at MWR Infosecurity, an F-Secure company, worked with Amazon to provide a fix for the vulnerability in the 2017 Echo, which was rolled out before the flaw had been announced. The device was then completely redesigned with new internal architecture for 2018.

Since Mark first reported on his hack in August of 2017, billions more connected IoT (Internet of Things) devices, which includes the Alexa, have been sold.

Barnes says that larger manufacturers like Amazon and Google—whose personal assistant rival to Alexa, Home, has seen phenomenal growth since the first Echo hack—have done an effective job of securing their mass-market devices, even if these tech giants may not be fully forthcoming about all the features of the devices.

Meanwhile, millions of connected devices from lesser-known manufacturers, including webcams and routers, remain vulnerable due to basic security weaknesses in their design. And criminals continue to seek and find ways to monetize this vast and growing sea of potentially vulnerable computing power.

[1] Alexa, are you listening? https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening/

INTRODUCTION

History may remember 2018 as the turning point.

A slow trickle of threats targeting the Internet of Things (IoT) that began at the beginning of the century became a steady stream. And these new threats, along with updated versions of existing malware that targets the IoT, seem to have found a way to monetize insecure devices.

Both Interpol and the FBI issued warnings about the dangers of vulnerable connected devices.

"All devices which can connect to the Internet – collectively called the 'Internet of Things' or IoT – are potentially at risk of a cyberattack," Interpol noted in a February 2018 release advising consumers to secure IoT devices the way they secure their PCs. [2] "Everyday personal items like video cameras, refrigerators and televisions can be used by cyber criminals for malicious means."

In August, the FBI stated that "routers, wireless radios links, time clocks, audio/video streaming devices, Raspberry Pis, IP cameras, DVRs, satellite antenna equipment, smart garage door openers, and network attached storage devices" could be hijacked for their computing power. And surely, this warning was correct.[3]

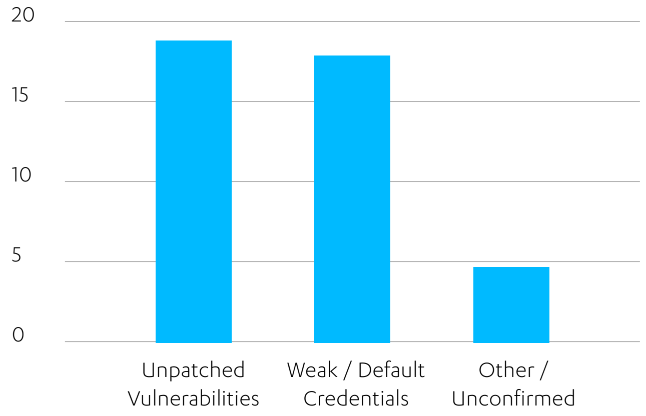
F-Secure Labs tracked the emergence of 19 new threats from January of 2018 through December – approximately doubling the number of IoT threats in the wild. Numerous IoT threats emerged focused on mining cryptocurrencies. Many of these threats were built off the leaked source code.

[2] Interpol warns IoT devices at risk https://www.scmagazineuk.com/interpol-warns-iot-devices-risk/article/1473202

[3] Cyber Actors Use Internet of Things Devices as Proxies https://www.ic3.gov/media/2018/180802.aspx

IoT DEVICES ARE "EASY PREY"

YEAR	COUNT
2002	1
2008	1
2009	1
2011	1
2014	3
2015	2
2016	5
2017	5
2018	19



The explosion of IoT devices in people's homes and offices is attracting attention from cyber criminals. And thanks to the security problems commonly found in these devices, they present attackers with low hanging fruit to pick. According to F-Secure Labs, threats targeting weak/default credentials, unpatched vulnerabilities, or both, made up 87% of observed threats.

In late 2018, F-Secure's network of reconnaissance honeypots servers observed a huge spike in threats targeting exposed telnet ports. Mirai uses this infection method to go after devices through default passwords. This explosion of attacks suggests that there is still plenty of "easy prey" out there and criminals are going after it.

Of the attacks observed by F-Secure's honeypots in 2018, 59%, were attacks targeting Telnet [4] – a trend F-Secure Labs attributes to the spread of Mirai malware.

THE FUTURE BEGINS NOW

Securing the smart home requires confronting the rampant vulnerabilities in IoT devices. In addition, the rising number of connected devices on home networks must be as secure as PCs and mobile devices. By inviting more and more tools into the home that can be used to track and observe consumers, security and privacy will play an increasingly crucial role in our lives.

The IoT remains a growing security and privacy risk to consumers, as well as a growing problem for businesses who provide consumers' access to the internet and accountable for any service interruption.

[4] Attack landscape H2 2018: Attack traffic increases fourfold https://blog.f-secure.com/attack-landscape-h2-2018/

IOT AND SMART HOME LANDSCAPE

The massive growth of the Internet of Things is the second great digital revolution of the last thirty years, as Mikko Hypponen often notes. The first revolution connected every computer to the internet. Now we are connecting almost everything else.[5]

The pace of "things" being connected is blistering—and unlike anything we've ever witnessed in human history. The World Wide Web was invented 30 years ago, in 1989. About seven years later, it became the largest online community in existence with 36 million users.[6] In 1999, Kevin Ashton used the term "Internet of Things" for the first time.[7] Cisco suggests the IoT was "born" sometime between 2008 and 2009.[8] By 2014, there were already more than 500 million "machine-to-machine" connections in use.[9]

The numbers vary depending upon how you define the IoT. The number of connected IoT devices probably passed the population of the earth, about 7.5 billion, some time in 2018 or early 2019. This number will likely triple by 2021.[10]

But regardless of how you define the IoT, the phenomenon of connecting almost "everything" is a trend that's transforming society. As a result, homes will continue to fill up with devices and appliances that connect to the internet. Cisco projects that beyond smartphones, tablets, and PCs, the average person in North America will have 14 networked devices by 2020 and a Western European will have nine.[11]

Personal assistants, such as Amazon Alexa or Google Home, exemplify the explosive growth possible for connected devices. The category barely registered in 2015. But by 2018 they could be found in nearly a quarter of American homes and 12% of European, according to an F-Secure consumer survey.[12]

The question is whether regulations that could protect consumers will come into effect fast enough to keep up with the IoT. There's a slight hope that may happen, but what happens next likely won't clean up the mess that's been made.

To get a sense of a scale of the problem, consider that a 10-year-old vulnerability discovered in 2018 left as many as half a billion IoT devices vulnerable.[13]

[5] Don't Kick The Robots" https://www.twice.com/blog/dont-kick-the-robots-they-might-kick-back

[6] "Web users reach 36 million now biggest user community" https://www.computerhistory.org/timeline/1996/

[7] "That 'Internet of Things' Thing" https://www.rfidjournal.com/articles/view?4986

[8] "The Internet of Things: How the Next Evolution of the Internet is Changing Everything" https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[9] "2017 roundup of internet of things forecasts" https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6d8a4f551480

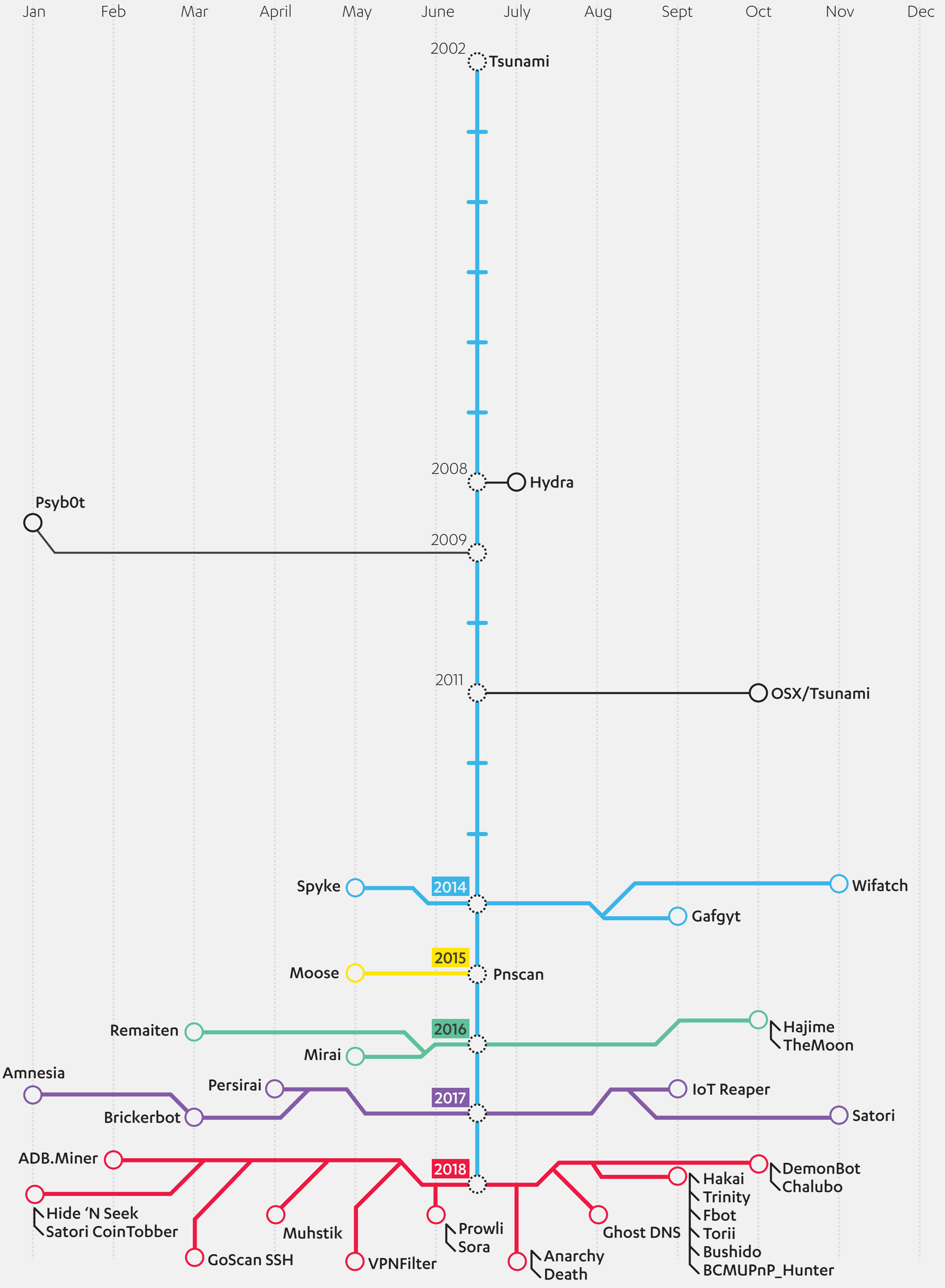
[10] "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating" https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[11] "North American Consumers To Have 13 Connected Devices" https://www.mediapost.com/publications/article/302663/north-american-consumers-to-have-13-connected-devi.html

[12] "Explosive IoT Growth Slowed by 'Early Adopter Paradox'" https://press.f-secure.com/2018/10/24/explosive-iot-growth-slowed-by-early-adopter-paradox/

[13] IoT Security Flaw Leaves 496 Million Devices Vulnerable At Businesses: Report https://www.crn.com/news/internet-of-things/300106806/iot-security-flaw-leaves-496-million-devices-vulnerable-at-businesses-report.html

A QUICK HISTORY OF IOT THREATS



The first Internet of Things threat that emerged nearly two decades ago looked a lot like the IoT threats observed for the next 12 or so years. But in the last few years, the development of malware targeting IoT devices has increased.

COMMON IOT THREAT CHARACTERISTICS

- Target embedded computers in devices like closed-circuit cameras, routers and DVRs.
- Use hard coded or default passwords to gain access.
- Co-opt computing power into a botnet for illegal purposes, including denial of service attacks, spam, and click-fraud.
- Build off of previous threats—in recent years, Mirai has been the foundation of an increasing number of malware targeting IoT devices.
- Spread increasingly more complicated payloads.

> Let's step back to near the turn of the millennium to take a look at a few key milestones in the development of IoT threats.

IN THE BEGINNING

In 2002, the first malware that could infect IoT devices was discovered.

Tsunami AKA Kaiten

- Spread manually
- Generally targeted Linux machines including IoT devices like routers and machines running BusyBox

In 2009, we saw a sneak preview of the IoT threats that we face today.

PsyB0t

- Spread automatically using 2,000 usernames and 13,000 passwords hard coded
- Executed "brute force" attacks through SSH or Telnet
- Hit router makers like D-Link and Telecom through its authentication bypass protocol

THE MODERN IOT THREAT ERA LEAKS OUT

In fall of 2014, Gafgyt emerged, but in 2015 its source code was leaked.

Gafgyt

- Another IRC backdoor, like its forefather Tsunami
- Used default and common passwords to carry out its infections
- By targeting multiple Linux architectures, it infected a wide variety of IoT devices, including BusyBox devices, closed-circuit television (CCTV) devices and many digital video recorders (DVR) devices

In 2015, attack payload started getting more complicated, targeting multiple platforms.

Moose

- Infected a device using brute force attacks through Telnet and set up a SOCKS and HTTP proxy
- Researchers found that the criminals used the zombie computers it coopted to engage in social

media click-fraud to build up fake followers and interactions such as likes and videos views [14]
- 86 percent of its traffic flows targeted Instagram
- Contained a "sniffer" that could monitor the infected machine to make sure it didn't belong to a highly secured system, like a bank or a government

IOT MALWARE BREAKS BIG

In 2016, we saw the first IoT threat that made headlines around the world.

Mirai

- Developed on top of the leaked Gafgyt source code
- Mirai took off when its code was posted to Github in fall of 2016
- Collaborative development of the threat made it much more potent
- Originally, 61 unique combinations of credentials used for infections. Within three months, that number had reached almost 500

In October of 2016 the botnet carried some of the largest denial of service attacks in history, taking down the internet for much of the East Coast of the United States. [15]

The same month of those historic Mirai attacks, malware with a new trick appeared.

Hajime

- In addition to abusing default passwords, this threat spread through the TR-069 protocol in routers used by many internet service providers

THE VULNERABILITY ERA

Almost a year later in September of 2017, there was another huge leap.

- **IoT_Reaper**
- Abandoned the use of hard-coded passwords to infect devices
- Instead used 10 known vulnerabilities in HTTP control interfaces, most of them in publicly facing IP and CCTV cameras
- Infected millions of devices

Hide N Seek

- Built off of the advances of IoT_Reaper
- Using the same vulnerabilities, it finds cameras to infect by randomly generating IP addresses
- Once servers are infected, it installed cryptominers, which generate virtual currency

[14] "Virus Bulletin 2018: Exposing the Social Media Fraud Ecosystem" https://threatpost.com/virus-bulletin-2018-exposing-the-social-media-fraud-ecosystem/137997/

[15] https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

ADB.Miner

- The first threat to use the bones of Mirai to target Android devices through the platform's debugger interface
- Also installed miners for virtual currency—specifically Monero

Meanwhile, new threats "forked" from Mirai and Gafgyt continued to appear, exploiting more and more vulnerabilities.

Fbot

- A Mirai variant that includes a blockchain-based DNS making it more difficult to track

Torii

- Utilizes exit nodes utilized by Tor's anonymizing software
- Perhaps the most advanced Mirai variant
- Multi-staged and uses at least six infection vectors.

NOW, THE BIG GUYS ARE IN THE GAME

In 2018, another milestone passed—an IoT threat that appears to have been sponsored by a nation-state.

VPNFilter

- Similarities to BlackEnergy malware led to speculation that it had been developed by Russian-backed actors to target the Ukraine
- Intercepted communication from SCADA systems used in manufacturing and the maintenance of infrastructure
- Sniffed out credentials
- Destroyed firmware built into the systems
- Targeted nearly every router on the market, nearly all of which have some sort of vulnerability or is susceptible to an attack using known or weak credentials

Vulnerable routers include models from Linksys, Mikrotik, Netgear, QNAP, TP-Link, Asus, D-Link, Huawei, Ubiquiti and ZT.

SMART HOME THREAT LANDSCAPE

"Whenever an appliance is described as being 'smart,' it's vulnerable," Mikko Hypponen, F-Secure's Chief Research Officer, tweeted in 2016. Hypponen's Law lays out theoretical risks of the compromise of the smart devices filling up our homes. [16]

Consumers and businesses are filling up with sensors, cameras, microphones, and multiple other devices that are accessible through the internet. Often, consumers and corporations are moving toward the trend of connecting everything with no sense of the potential risks they're voluntarily bringing into the spaces where they spend most of their lives.

[16] "Hypponen's Law and the Future of the IoT" https://blog.f-secure.com/what-hypponens-law-means-for-the-future-of-the-iot/

VULNERABLE GATEWAYS

At this point, the most vulnerable device in the home may be the one that connects most of the other devices to the internet. More than 8 out of 10 home and office routers were vulnerable to hacking, according to a 2018 study by the American Consumer Institute. [17] This included five of the six major brands. It's entirely possible that a router might have been hacked without the user even knowing it. With a technique called DNS hijacking, hackers can redirect traffic to a phishing website, where consumers may offer up a credit card number or login credentials.

THE RISKS

The biggest threat consumers face when using the IoT is the automatic infection of devices. There are multiple ways to attack the control interfaces of these devices, including HTTP, SSH and Telnet ports.

Public facing devices such as routers, cameras and DVRs remain the most obvious targets for criminals. But with more and more appliances becoming connected, embedded computers in washing machines and refrigerators are nearly as vulnerable. At the moment, the biggest problem is the device instability that results from these threats.

These risks can feel nebulous, but you don't have to look hard to see that they are real.

TARGETING THE MOST VULNERABLE

To get a sense of the immense privacy issues that can result from IoT or connected devices being compromised, consider victims of domestic abuse. In February of 2019, Eva Galperin, Director of Cybersecurity at the Electronic Frontier Foundation, tweeted, "Dear Past Me: Future You will spend her weekends driving for an hour to pay a house call to a woman whose abusive partner was spying on her through her Nest. Stock up on Xanax." [18]

The New York Times did over 30 interviews with survivors of domestic abuse and the professionals who work with them in the fall of 2018, and found that abusers are using smart devices to harass their victims.

"Abusers — using apps on their smartphones, which are connected to internet-enabled devices — would remotely control everyday objects in the home, sometimes to watch and listen, other times to scare or show power," the story noted. [19] "Even after a partner had left the home, the devices often stayed and continued to be used to intimidate and confuse."

[17] "ThreatList: 83% of Routers Contain Vulnerable Code" https://threatpost.com/threatlist-83-of-routers-contain-vulnerable-code/137966/

[18] https://twitter.com/evacide/status/1094809216521359360

[19] "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse" https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

THE INTERNET OF SH*T

The bio of the popular Twitter account @ internetofshit reads "whatever, put a chip in it." [20]The feed is dedicated to the ridiculous things that happen when everything goes online. A quick scan of the account and you might see a lawnmower that tracks the user to reveal the best time to mow or hacks people have to do to make their "smart" doorbells work or the already classic case of Adapt BB—the Nike "smart" sneakers that stopped working after a bad update.

"Some report that either the left or right sneaker fails to pair after attempting to update them through the companion Android app," The Verge reported. [21] "That means the sneaker can't be tightened or properly worn. Some users say the update caused the motor to stop functioning, too, so even the physical buttons don't work."

THIS NEEDS TO WORK

This smart home threat landscape veers quickly from the terrifying—domestic harassment through a thermostat—to the absurd—smart sneakers. But the dependency on the internet being built into our homes is no joke. A thermostat that does not operate in extreme temperatures, a hacked webcam that enables actual theft or harassment, an alarm system that needs to protect your family from smoke or other threats—these are all deadly serious problems.

And on a practical level, the internet still needs to function reasonably well while it's being used, even for bandwidth-intensive activities like streaming video on several different devices at once. Instability due to insecure devices may be easy to blame on the manufacturer, but providers of internet connections know they're going to get the blame when a home network is slowed to a crawl by cryptominers.

[20] https://twitter.com/internetofshit

[21] "Nike says it's 'actively working' to fix its broken smart sneakers" https://www.theverge.com/circuitbreaker/2019/2/21/18234615/nike-adapt-bb-fix-android-bug-firmware-update-patch

REGULATION AT LAST?

"Many IoT device vendors have little to no experience in building internet-connected devices," Mikko Hypponen, F-Secure's Chief Research Officer, and Tomi Tuominen, F-Secure's Practice Leader, wrote in the F-Secure State of Cyber Security 2017. "They build IoT devices to be cheap and to work, but not to be secure." [22]

There is a simple reason that manufactures get away with shoddy security—no one stops them. No regulator has the power to dictate the standards needed to address common security issues. So consumers are left to make security assessments on their own. Often, they just end up buying the cheapest device on the market.

In January of 2018, "Pinning Down the IoT" a Cyber Security Research Institute report into the Internet of Things sponsored by F-Secure stated, "In its current form the Internet of Things (IoT) represents a considerable threat to consumers, due to inadequate regulations regarding its security and use." [23]

This is mostly true a year later. But there is some new hope. After a decade filled with an explosion of inferior devices rushed to market without ample regard for security, manufacturers have begun to catch up with the risks. Many router manufacturers have implemented updated policies that reduce the number of vulnerable devices that act like open doors into the so-called "smart home." The use of default or weak credentials is finally diminishing after more than a decade of widespread adoption of this industry-wide "worst practice."

Meanwhile, more experienced manufacturers, like Google and Amazon, have hardened their smart home devices with the help of billions of dollars in assets and ethical hackers like Mark Barnes. These brand names have thus far remained largely immune to the IoT attacks that have infected millions of routers, cameras, and digital recording devices.

This has helped drive their adoption despite privacy risks. These devices could potentially record everything we do and say, even when consumers least suspect it. For instance, Google was forced to announce in early 2018 that its "smart" Nest security system included a microphone that was not disclosed to consumers. [24]

But there is much more that needs to be done. Several pieces of legislation have been introduced in the United States Congress. [25] These bills range from producing more consumer education about IoT devices, to placing requirements on IoT devices for government use, to establishing standards for the devices themselves.

In October of 2018, the UK released a "first of its kind" IoT security code of practices that lays out 13 guidelines that manufacturers should adhere to in order to safeguard their devices and customers.
These are positive but non-binding steps. A solution that would demand radical transformation for the industry already has a foothold in the European Union.

"I think GDPR-wise, the GDPR could be extended to actually cover the IOT devices or some other regulation could come in place that would extend the GDPR to actually cover these IOT devices as well," Laura Kankaala, F-Secure Security Consultant, said last year on F-Secure's Cyber Security Sauna podcast.[26]

[22] "Should You Fear the IoT_Reaper?" https://blog.f-secure.com/should-you-fear-the-iot_reaper/

[23] "Pining Down the IoT" https://fsecurepressglobal.files.wordpress.com/2018/01/f-secure_pinning-down-the-iot.pdf

[24] "Users alarmed by undisclosed microphone in Nest Security System" https://arstechnica.com/gadgets/2019/02/googles-nest-security-system-shipped-with-a-secret-microphone/

[25] "Regulating the Internet of Things" https://www.rfidjournal.com/articles/view?18038

[26] "Supply chain attacks, IoT exploits, and other trends coming in 2019" https://blog.f-secure.com/supply-chain-attacks-iot-exploits-trends-coming-2019/

Given the data flows through our IoT devices, smart phones, and various cloud services, a GDPR-style solution seems inevitable. But it also seemed inevitable there would be some sort of regulation of these devices before there were more of them than there are people on earth. Yet here we are.

WHAT'S NEXT?

For right now, we should expect more of the same.

The IoT threats we face are most likely to focus on using hijacked resources to help launch denial-of-service attacks and mining for virtual currencies. F-Secure Labs has seen some evidence that cryptomining slowed slightly as the year began, possibly because research suggests criminals aren't finding the tactic to be very profitable. [27] But some experts expect this trend to reverse, especially as cryptocurrency prices fall and increased mining is needed to make up for losses. [28]

For smart homes, privacy concerns will likely dominate security issues. Using the massive amounts of information "smart home" devices collect about their users, large corporations could target us in ways we can't even imagine. For instance, news that Roomba, iRobot's Wi-Fi connected vacuum robot, was creating maps of people's homes skyrocketed the manufacturer's stock price. Clearly investors have a better idea of what corporations might do with this data than the general public.

And a look at how hacking groups have successfully targeted businesses through IoT infrastructure, include things like cardiac devices and aquariums, gives us a hint at how hackers may go after high-value targets using IoT or smart home devices.

CONCLUSION

Connecting PCs together in the 1990s, without ample security, made cyber crime a profitable endeavor. Fast forward to today, and it's become a billion-dollar industry. Instead of learning from these mistakes, we seem to be repeating them as we connect almost everything else to the internet.

Deploying massive amounts of computing power without prioritizing security and privacy has created a new target that criminals are just beginning to exploit. This requires immediate action by manufacturers, regulators and everyone responsible for connecting people to the internet. Because when these threats turn our technologies against us, no one can say that we weren't warned.

[27] "Web-based Cryptojacking in the Wild" https://arxiv.org/pdf/1808.09474.pdf

[28] "Why cryptojacking will become an even larger problem in 2019" https://www.techrepublic.com/article/why-cryptojacking-will-become-an-even-larger-problem-in-2019/

ABOUT F-SECURE

Nobody knows cyber security like F-Secure. For three decades, F-Secure has driven innovations in cyber security, defending tens of thousands of office, homes, and millions of people. F-Secure shields enterprises and consumers against everything from advanced cyber attacks and data breaches to widespread ransomware infections. F-Secure's AI-driven solutions also help to protect the connected devices and homes of your customers. The unique combination of technology and world-class Business Services supporting the entire customer lifecycle is what makes F-Secure an excellent fit for the service provider channel. F-Secure's products are sold globally by more than 200 service providers and thousands of resellers.

www.f-secure.com/connected-home-security

F-Secure®