IoT in the enterprise 2020:

Shadow IoT emerges as security threat

by Zscaler™ ThreatLabZ™
February 2020

zscaler™

Overview

The volume of legitimate enterprise IoT traffic is rising, but an analysis of the IoT data stream hitting the Zscaler™ cloud has also uncovered a troubling surge in the amount of unauthorized IoT traffic, or shadow IoT.

83% of IoT transactions are happening over plain text channels, with only 17% using secure (SSL) channels.

The volume of traffic generated by both authorized and unauthorized internet-of-things (IoT) devices is skyrocketing, adding to enterprise security risks, according to an analysis of cloud traffic conducted by Zscaler.

In May 2019, when the Zscaler ThreatLabZ research team released its initial report on IoT traffic generated by its enterprise customer base, the Zscaler cloud was processing 56 million IoT transactions a month. By February 2020, that number had soared to 33 million transactions a day and to an astounding **1 billion IoT transactions per month**, which amounts to a 1,500% increase. (Zscaler processes 85 billion internet transactions in a single day, so 33 million IoT transactions represents just a fraction, albeit a rapidly growing fraction, of total traffic.)

By February 2020, the Zscaler cloud was processing 33 million IoT transactions per day and an astounding 1 billion IoT transactions per month.

Just as traffic volumes have surged, so has the amount of IoT-based malware. Zscaler was blocking 2,000 pieces of IoT-based malware per month in May 2019; that number has increased seven-fold to 14,000 malware attempts blocked per month.

One of the key findings in this latest analysis is that as enterprises have embraced mobility and always-on connectivity for employees, the lines have blurred between company-owned and privately owned devices, and between the workplace and the home. In many cases, enterprise IT teams might not even be aware of some of the devices generating IoT traffic, and this new culture of shadow IoT is creating new IoT-based attack vectors for cybercriminals.

©2020 Zscaler, Inc. All rights reserved.

The top IoT device categories identified by Zscaler include authorized devices such as data collection terminals, digital signage media players, industrial control devices, medical devices, networking devices, payment terminals, and printers.

But the analysis also showed enterprise traffic generated by unauthorized IoT devices such as digital home assistants, TV set-top boxes, IP cameras, smart home devices, smart TVs, smart watches, and even automotive multimedia systems.

What this tells us is that employees inside the office might be checking their nanny cam over the corporate network. Or using their Apple Watch to look at email. Or working from home, connected to the enterprise network, and periodically checking the home security system or accessing media devices. Even more troubling from a security perspective is the fact that roughly 83% of IoT-based transactions are happening over plain text channels, whereas only 17% are using SSL. The use of plain text is risky, opening traffic to sniffing (for passwords and other data), eavesdropping and man-in-the-middle attacks, and other exploits, which is why it is no longer used for the vast majority of web and application traffic.

Enterprise IoT traffic included personal digital home assistants, TV set-top-boxes, and even automotive multimedia systems.

Attackers are certainly aware of the potential vulnerabilities. In the case of the Mirai botnet of 2016, attackers exploited the fact that consumers rarely change the default password on IP cameras and home routers and launched a denial-of-service attack that took down a big chunk of the internet. And new exploits that target IoT devices are popping up all the time, such as the RIFT botnet, which looks for vulnerabilities in network cameras, IP cameras, DVRs, and home routers.

The growth of IoT shows no signs of abating. According to IOT Analytics, there were more than 4.7 billion things connected to the internet in 2016. By 2021, that number will increase to more than 11 billion and, by 2025, it is estimated that the number will hit 21 billion. Market research firm IDC predicts that IoT spending will surpass the $1 trillion mark in 2022, a 15% increase over 2018's $646 billion.

©2020 Zscaler, Inc. All rights reserved.

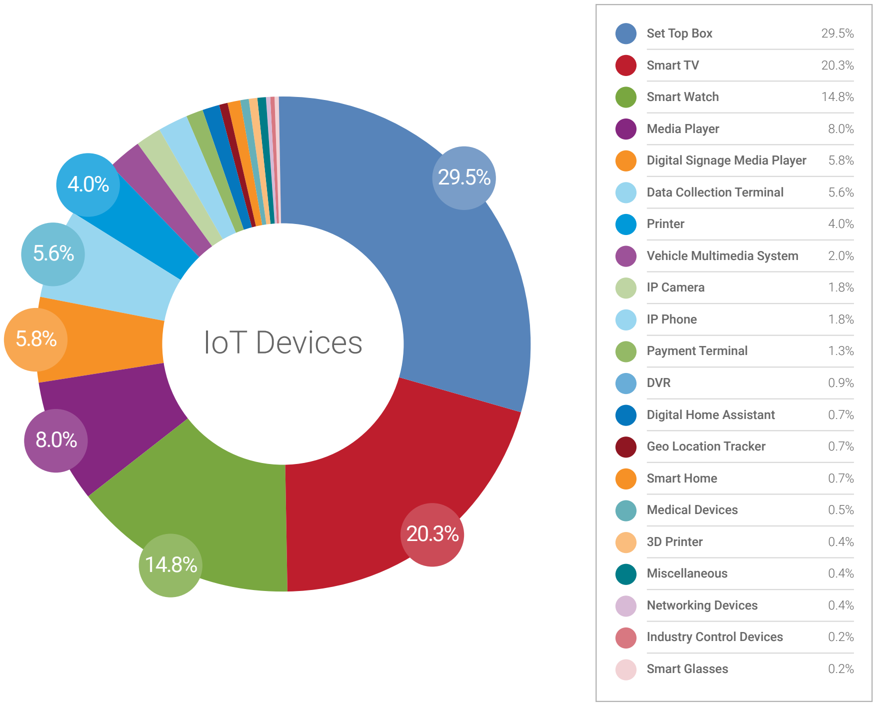
In response to the growing threat posed by shadow IoT, enterprise IT should focus on gaining visibility into the existence of unauthorized IoT devices that are already inside the network, putting IoT devices on a separate network, restricting access to the IoT device from external networks, changing default credentials, requiring strong passwords, and applying regular security and firmware updates.

Here are some of the key results based on an analysis of nearly 500 million transactions from more than 2,000 organizations over a two-week period. Of those transactions, the analysis revealed a total of **553 different IoT devices in 21 categories from 212 manufacturers.**

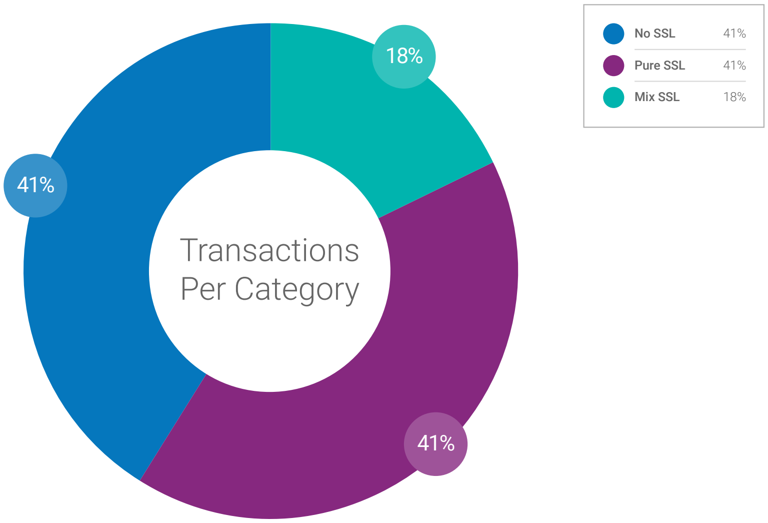
The analysis revealed a total of 553 different IoT devices in 21 categories from 212 manufacturers.

IoT devices and transaction volume in the cloud

When the researchers looked at the total number of devices and drilled down to build an inventory of IoT devices sending traffic to the Zscaler cloud, consumer devices topped the list. The category with the highest number of individual devices was far and away TV set-top boxes, which enable analog television sets to receive digital broadcasts (29.5%), followed by smart TVs at 20.3%. In other words, two categories accounted for roughly half of all devices. Coming in third were smart watches at 14.8%, followed by media players at 8%, digital signage media players at 5.8% and data collection terminals at 5.6%.



©2020 Zscaler, Inc. All rights reserved.



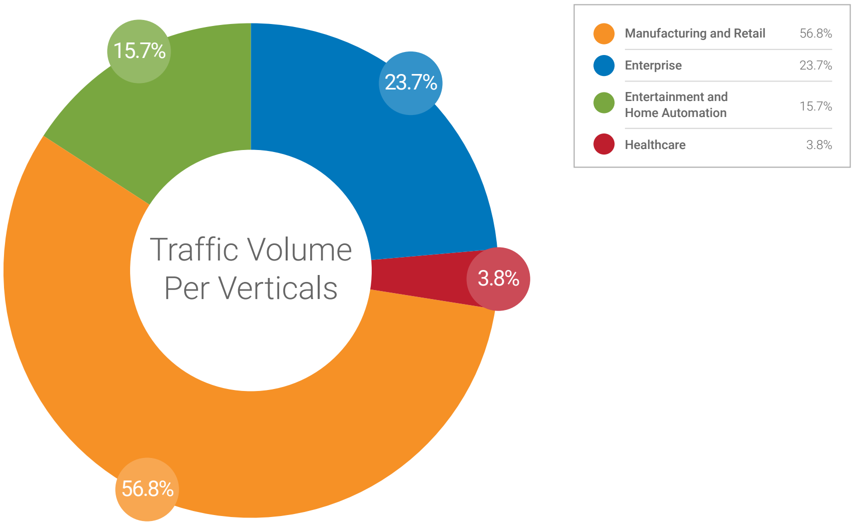
However, when it comes to the total number of transactions, business process IoT devices dominated. In fact, the majority of IoT transactions were conducted with data collection terminals (56.8%), which are wireless barcode readers used in manufacturing, engineering, logistics and warehousing applications. These were followed by printers at 16%, media players at 7.7%, and digital signage media players at 7.1%. Meanwhile, it's astounding to see so many of these IoT devices use no SSL at all (41%). This would be an enormous blind spot in an organization with a more legacy approach to networking and security since organizations should be inspecting all encrypted traffic. There is deeper analysis of this data later in the report.

The top 10 destinations (where the device traffic was being sent) by unique device type were the United States, Ireland, Japan, Germany, France, China, United Kingdom, Netherlands, Canada, and Poland. And the top destinations for all IoT traffic were the United States (73%), Australia (11%), Ireland (6%), Mexico (3%), South Korea (2.7%), Japan (1.1%), China and Namibia (1%), and Netherlands (0.7%).

Traffic volume by industry

Manufacturing and retail industries generated the most IoT traffic volume at 56.8%, followed by enterprise at 23.7%, entertainment and home automation at 15.7%, and healthcare at 3.8%.

©2020 Zscaler, Inc. All rights reserved.



In manufacturing and retail verticals, the Zscaler team identified 57 different device types from 20 manufacturers, including 3D printers, geolocation trackers, industrial control devices, automotive multimedia systems, data collection terminals, and payment terminals.

Specifically, the team saw 3D printers from Ultimaker; geolocation trackers from Garmin, Aguri, and Prestigio; industry control devices from Siemens; data collection terminals from Zebra, Honeywell, and Coppernic; and payment terminals from Elo, SUNMI, and Telepower. In addition, the logs showed automotive multi-media systems from manufacturers like Tesla, Honda, Autel, and MaxiSys.

The enterprise vertical included devices such as digital signage media players, digital video recorders, IP cameras and phones, printers, and networking devices.

This traffic was made up of 80 different IoT devices from 39 manufacturers. Among digital signage media players were brands like BenQ, BrightSign, Navori, ViewSonic, and Phillips. The most prevalent DVRs were from TVT, EverFocus, and DIRECTV. There were IP cameras and IP phones from Axis, Foscam, Samsung, Yealink, and Cisco, plus networking devices from Ixon and NetBiter.

In healthcare, IoT traffic that hit the Zscaler cloud came primarily from three manufacturers: GE Healthcare, Abbott Laboratories, and HOLOGIC.

©2020 Zscaler, Inc. All rights reserved.

In the entertainment and home automation category, devices included digital home assistants, media players, set-top boxes, smart glasses, smart home devices, smart TVs, and smart watches, with a total of 420 devices from 150 different manufacturers.

Digital home assistants included brands such as Amazon, Apple, and LG; media players were from Sonos, Roku, Pioneer, Bose, Aluratek, and ZTE; and there were set-top boxes from Technicolor, Roku, Xiaomi, Minix, Amazon, and Airtel.

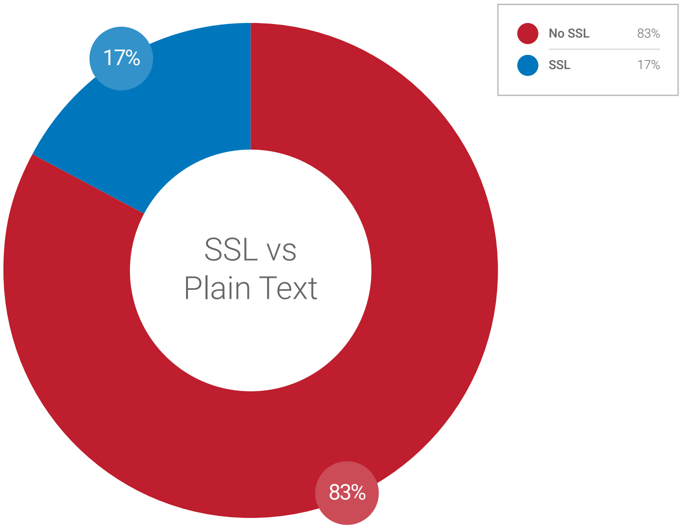
In the "smart" category, there were smart home systems from Samsung, Skybell, and Ring; smart TVs from LeTV, Sony, Samsung, LG, Hisense, Panasonic, Phillips, Sharp, and Xiaomi; smart watches from Apple, Fossil, Pebble Time, LG, Samsung, Lemfo, Mobvoi; and smart glasses from Google.

Security and privacy concerns

The analysis showed that some devices are not following proper security practices, which makes them vulnerable to crafted attacks. What follows are the security issues Zscaler researchers most frequently observed:

1. Plain-text HTTP communication to server for firmware or package updates
2. Plain-text HTTP authentication
3. Use of outdated libraries
4. Weak default credentials

When looking into how many devices were transacting in plain text and how many were doing so over encrypted channels, the team saw that around 83% of transactions were happening over plain-text channels, whereas only 17% used secure (SSL) channels.



Even so, all devices used a mix, with some transactions occurring over SSL and some over plain text. There were no devices that used all SSL or no SSL at all. Inspecting all SSL traffic is critical to protect the enterprise. Vast numbers of malicious files delivered by SSL including ransomware families, trojans of any variety and other command and control payloads.

©2020 Zscaler, Inc. All rights reserved.

*Each quarter, the Zscaler cloud blocks **around 42,000 transactions** for IoT-based malware and exploits. The top malware families are Mirai, Gafgyt, Rift, Bushido, Demonbot and Pesirai. The top destinations connected by IoT malware families and exploits are United States, UK, Russia, Netherland, and Malaysia.*

Surprising devices found in the cloud

Zscaler identified a number of unique and interesting IoT devices connecting to the Zscaler cloud:

- **Smart refrigerator:** A smart refrigerator from Samsung was seen connecting to the cloud. This appliance has the ability to stream music, videos, and content from the owner's phone to a screen on the refrigerator door.
- **Music furniture:** This is a combination table lamp and smart media player device named Symfonisk. It's made by Ikea and Sonos.
- **Automobiles:** Tesla and Honda automobile media players connected to the Zscaler cloud.
- **Wi-Fi memory cards:** Wi-Fi memory cards from Eye Fi, generally used in cameras for storing and sharing photos over Wi-Fi, were sending traffic through the Zscaler cloud.

The surge in IoT devices shows no signs of slowing down and the presence of shadow IoT highlighted in this report should serve as a wake-up call to enterprise security professionals. Just as companies learned to create policies and to apply management and security controls to BYOD devices, they need to start paying that same level of attention to shadow IoT.

©2020 Zscaler, Inc. All rights reserved.

Shadow IoT: So What?!

This research from Zscaler ThreatLabZ sheds light on the rising risks of Shadow IoT creeping into the enterprise. Now, what can be done about it?

You can't attack what you can't see, of course, but by the same logic you cannot protect against devices you don't even know are on your network. So, you first need the visibility into your entire infrastructure to shine a light on shadow IoT devices. Organizations also should be considering a zero trust approach that ensures any communication between devices and people is with known entities and is within your organization's policy. Finally, if possible, urge action at the governmental level to have a common set of policies and regulations with respect to the development and security of IoT devices.

You can read more in-depth takeaways in the Zscaler blog,
Shining a Light on Shadow IoT to Protect Your Organization.

Research © 2020 ThreatLabZ, the research division of Zscaler Inc. All rights reserved. Zscaler™ is either (i) a registered trademark or service marks or (ii) a trademark or service marks of Zscaler, Inc. in the United States and/or othercountries. Any other trademarks are the properties of their respective owners.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com