OpenDNS

The 2015 Internet of Things in the Enterprise Report: **Executive Summary**

Security for the way the world works today.

About OpenDNS

OpenDNS is a leading provider of network security and DNS services, enabling the world to connect to the Internet with confidence on any device, anywhere, anytime. The Umbrella cloud-delivered network security service blocks advanced attacks, as well as malware, botnets, and phishing threats regardless of port, protocol, or application. Its predictive intelligence uses machine learning to automate protection against emergent threats before they can reach customers. OpenDNS protects all devices globally without hardware to install or software to maintain. For more information, please visit: www.opendns.com.

About OpenDNS Security Labs

At OpenDNS Security Labs we thrive on continual innovation. But we don't simply look at data from new threats and ask ourselves, "If we had known that before, what would we have done differently?" We look at our extensive data collection network built on top of the largest security infrastructure and predict what's coming next. We're a team of world-class engineers, mathematicians, and security researchers, and we're taking an innovative and proactive approach to security research. More than any other area of technology, we see history repeat itself most often in information security. The way we have traditionally defended against malware has become a cycle: new technologies are created and adopted, attackers leverage the opportunity to expand the attack surface, and security solutions are released in reaction to the latest threats. But this method is tired, and we can do better. Our goals are simple: to continually innovate ahead of the pace of technology change and build the best security protection and security delivery network platform possible without compromising performance or productivity.

OpenDNS Security Labs authored this report. Any questions about the methodology should be addressed to Andrew Hay, Director of Security Research, OpenDNS, andrew.hay@opendns.com.

Preamble

It is a popular belief that security companies and researchers report on events in a manner that is over-hyped, exaggerated, and miscommunicated. Often, that's true. Some security companies seek to grab the industry's attention with sensational blog headlines. We can say with confidence that we do things differently. The analysis and findings we will present are driven by evidence and technology facts. The report will not include hearsay, rumors, or obvious predictions around events or circumstances. When there is cause for alarm, we present reason and advice based on facts stemming from our data. We aim to provide proof-points, relevance, and pervasive evidence with our research, and you can hold us to that.

More information about the core values and beliefs of OpenDNS Security Labs can be viewed on our blog at https://labs.opendns.com/about-us/.

We acknowledge that security research is often loaded with fear, uncertainty, and doubt (FUD). This report is about visibility into IoT communications and highlights potential problems before the connected landscape becomes unmanageable. This report is NOT FUD.

Visibility is a foundation of security and is critical in understanding the organization's security posture and overall risk profile. One cannot measure risk without first having visibility into what is happening.

Privacy Statement

Due to the size of the data, with often more than 70 billion daily DNS queries, OpenDNS Security Labs chose to limit the scope of research by performing statistically relevant sampling of the data at regular intervals on the 15th day of February, March, and April in 2015. All data was meticulously sanitized so as not to reveal client IP addresses or individual company names. Should you have any concerns regarding the privacy or security of the analyzed data or employed methodology, please email andrew.hay@opendns.com.

Vendor Outreach

During our research we reached out to several vendors to foster an environment of sharing and collaboration. Unfortunately, Western Digital and ioBridge did not return our calls, emails, or acknowledge our social media outreach attempts. Axeda, a PTC company, and mnubo, however, were far more open to working with us on our findings. It should be noted, however, that no new exploitation details for the surfaced vulnerabilities have been released that have not otherwise been published previously.

Key Findings

Though our report discovered an extensive number of concerning and important findings, the following seven are the most significant.

1. IoT devices are actively penetrating some of the world's most regulated industries including healthcare, energy infrastructure, government, financial services, and retail.
2. Our analysis identified three principal risks that IoT devices present in protecting network environments with IoT devices: **(1)** IoT devices introduce new avenues for potential remote exploitation of enterprise networks; **(2)** the infrastructure used to enable IoT devices is beyond both the user and IT's control; **(3)** and IT's often casual approach to IoT device management can leave devices unmonitored and unpatched.
3. Some infrastructures hosting IoT data are susceptible to highly-publicized and patchable vulnerabilities such as FREAK and Heartbleed.
4. Highly prominent technology vendors are operating their IoT platforms in known "bad Internet neighborhoods," which places their own customers at risk.
5. Consumer devices such as Dropcam Internet video cameras, Fitbit wearable fitness devices, Western Digital "My Cloud" storage devices, various connected medical devices, and Samsung Smart TVs continuously beacon out to servers in the US, Asia, and Europe–even when not in use.
6. Though traditionally thought of as local storage devices, Western Digital cloud-enabled hard drives are now some of the most prevalent IoT endpoints observed. Having been ushered into highly-regulated enterprise environments, these devices are actively transferring data to insecure cloud servers.
7. And finally, a survey of more than 500 IT and security professionals found that 23 percent of respondents have no mitigating controls in place to prevent someone from connecting unauthorized devices to their company's networks.

Is IoT a Problem for the Enterprise?

The goal of this research study was simple: use a data-driven methodology to explore the potential security risks surrounding the Internet of Things (IoT) within enterprise networks.

As a highly covered topic, a lot of hypothetical discussion surrounds the potential impact of IoT. The lack of reporting using concrete data means that IT departments around the world base decisions on surveys, expert predictions, and conference talks that explore specific devices and possible scenarios.

OpenDNS Security Labs set out to create the first comprehensive look at the current state of IoT devices. We strongly encourage you to **read the full report** as it dives into much greater detail about the methodology and specific findings. This condensed version of the full report discusses the key findings from an executive-level vantage point.

It's worth noting that the intention of this report is not to scare or shock the public. It is meant to provide an unprecedented data-driven view of IoT based on real data that security professionals can use to gain better understanding, help educate company business decision makers, and to plan for an IT security future that includes ubiquitous IoT devices.

IoT Devices Are Active in Highly Regulated Industries

The data we gathered shows significant permeation of IoT devices across market verticals that are highly regulated or that manage sensitive data. The top three verticals are education, managed service providers, and healthcare. Also discovered in the top 15 verticals are energy infrastructure (8th), manufacturing (10th), government (12th), and financial services (13th).

These market verticals are considered to be highly regulated, because the data they manage and store is highly sensitive. These are the verticals that should have the strongest security practices in place, as well as strict compliance requirements. A presence of IoT within these industries is a cause for concern, especially given that responses to a survey sponsored by OpenDNS suggest there is a misunderstanding of IoT and a large margin of unpreparedness for it.

IT Is Unprepared but Still Deploying IoT Gadgetry

OpenDNS conducted a survey of 500 IT and security professionals and 500 consumers between March and April 2015. The aim was to better quantify the understanding of IoT, the potential threats connected devices pose, and the current approach enterprises are taking to address the problem. The result is an interesting disclosure of the current sentiments and behaviors around IoT devices.

An increase of employee-owned IoT devices forces IT to rely more heavily on user behavior to reduce their impact on company networks. Even so, because of the risks involved, technical enforcement of IoT policies is imperative. The survey results show that enterprises have made attempts to address the rapid growth of IoT devices on their networks, with almost 75% having set a defined policy. Yet only 35% of consumers report being aware of any such policy at their companies.

Responses to three questions explicitly identify the discrepancies in IT's preparedness for a proliferate IoT presence. More than 60% of IT professionals responding to our survey said they have plans to deploy more IoT enabled devices. This stands in stark contrast to the current state of mitigating controls aimed at IoT vulnerabilities.

When asked, 23% of IT respondents admitted having no mitigating controls in place that would prevent someone from connecting unauthorized devices to their company networks. And only 35% have a separate WiFi network for unapproved devices.

These three figures represent a significant gap between the number of enterprises with mitigating controls for IoT and the number of devices deployed. According to our survey results, this gap is also set to widen substantially in the short term.

IoT Devices Beacon Out Incessantly

From our in-depth analysis of specific devices and their network behavior, it's clear that today's crop of devices are beaconing (repeatedly using their connectivity to call "home") for a variety of reasons.

While we can't speak to how manufacturers and IoT service providers use the data from this type of activity, some of the motivations behind the behavior could be:

- Running updates for app and current info (e.g., "latest videos" in a YouTube app)
- Checking for system updates
- Monitoring usage
- Backing up device data

Specifically, our analysis of Samsung Smart TVs found this beaconing behavior to be common. While the issue of voice recognition has been widely discussed, our research also shows that these systems regularly beacon out to several external network locations when sitting idle (with no user interaction).

Additionally, we found indications that Smart TVs may be communicating with legacy infrastructure that uses an untrusted security certificate, opening this avenue of communication to several well-known attacks.

Persistent Internet connectivity and beaconing behaviors were also observed in the Dropcam line of cameras, and the Nest thermostat. Despite the concerns Matt Burrough and Jonathan Gill raised in 2013 in a university research paper about the Nest and other thermostats, they continue to maintain persistent connections to the Internet, even in hibernate mode.

While it's important to recognize that this behavior isn't inherently malicious, it does pose a risk for the user. Attackers can potentially monitor these devices for network activity and discover usage patterns about its owner. This type of beaconing also presents an additional attack surface for criminals to target if a device-specific exploit is discovered.

IoT Infrastructure Is Vulnerable

Untrusted Smart TV security certificates were not the only security issue we discovered.

Leveraging the unique OpenDNS dataset (OpenDNS processes about 2% of the Internet's DNS requests), we were able to conduct a neighborhood analysis of the ASNs (autonomous system number) hosting IoT infrastructure.

While most IoT infrastructure is running on top of modern service providers like Amazon, SoftLayer Technologies, Verizon Business, and others, OpenDNS Security Labs discovered that some providers are also hosting malicious domains.

While the IoT infrastructure is not an immediate risk by being in a network neighborhood with malicious domains, it is common for attacks to move horizontally within a network. This finding highlights the need for device manufacturers to stay with top-tier service providers for these supporting applications. For an enterprise to fully understand the risks an IoT device presents, it is key to research not only the device itself, but also its supporting network infrastructure.

An example of risky network infrastructure is our discovery that several IoT infrastructures are susceptible to highly-publicized and patchable vulnerabilities.. During our research, we discovered services vulnerable to Heartbleed (CVE-2014-0160), FREAK (CVE-2015-0204), POODLE (CVE-2014-3566), and a number of incorrectly configured SSL connections.

The most concerning example of precarious IoT infrastructure came from our analysis of Western Digital devices with MyCloud capability. Thirty of the 70 domains associated with the MyCloud service were found to be vulnerable to FREAK, which puts the user's data directly at risk.

Conclusion

While many security experts have authored warnings about the Internet of Things, the full "2015 Internet of Things in the Enterprise" report is filled with data proving that these connected devices put enterprises at risk for attack.

An alarming number of highly regulated industries show a presence of IoT tools and gadgets beaconing out to the Internet. Some of these devices send traffic to malicious network neighborhoods, and some gather data or beacon out even when not in use. Hackers and data thieves can use this device behavior to study usage patterns, stage an attack on an unpatched device, or use the device's insecure infrastructure to move horizontally into an enterprise's network.

We describe certain market verticals as highly regulated because the data some companies we found utilizing IoT devices are exceedingly sensitive. Needless to say, adding more attack vectors for hackers to exploit in these industries is a risky practice. It is critical that IT and security professionals charged with protecting these networks get out in front of this growing issue. IoT-enabled devices should be regarded and managed as equipment connected to the Internet, as well as closely monitored to provide warning signs of an attack.

For more specific findings and recommendations for protection, read our full *The 2015 Internet of Things in the Enterprise Report*. It includes detailed analysis on the types of devices we studied, the industry verticals hosting them, and patterns of unsafe behavior we observed, plus full results of our survey.

OpenDNS

OpenDNS, Inc. | www.opendns.com | 1.877.811.2367

052915