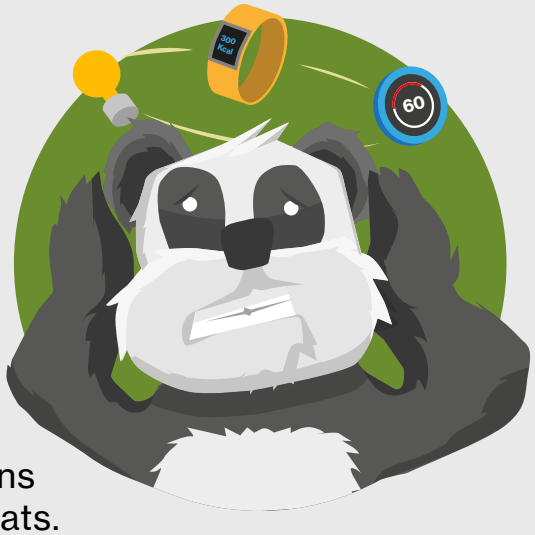
verizon

Data Breach Digest

IoT Calamity: the Panda Monium



Security is often an afterthought when it comes to IoT (Internet of Things) solutions – and that means devices are often vulnerable to a wide array of threats.

The Impact of IoT

IoT possesses a huge potential to forever change the way we interact with the world through technology. The proliferation of IoT devices essentially leads to increased automation, big data analytics, and artificial-intelligence-based decision making in our daily lives. An IoT solution requires a detailed and comprehensive security and privacy framework. This is an area that unfortunately still needs a lot of work on design – as well as a substantial impetus on collaboration by the IoT market players on the underlying security.

Despite the fact that we are in a hyper-connected world, the security of the IoT is still at times somewhat of an afterthought. The main issue is that most firms do not realize that components behind the IoT's agile innovation can easily go wrong, and can have a far greater impact than what can be seen in the traditional IT landscape. IoT devices are usually constantly connected to the internet and may not be looked at from a security perspective, thus leaving them vulnerable to a variety of attacks. This makes IoT devices an ideal target for being conscripted into a botnet army.

What is IoT?

IoT, the "Internet of Things," is a term that describes a network of physical objects connected to the internet. These may be discrete items like light bulbs or larger systems like building automation solutions. Embedded in each device are electronics capable of network connectivity along with sensors or other features.

The Case of the Botnet Barrage

Senior members of my university's IT Security Team rotated weekly as on-call "Incident Commanders" in the event that a response was needed. This week was my turn and as I sat at home, my phone lit up with a call from the help desk. They had been receiving an increasing number of complaints from students across campus about slow or inaccessible network connectivity. As always seemed to happen, the help desk had written off earlier complaints and it was well after 9 PM when I was finally pulled in.

> "IoT devices are an ideal target for being conscripted as part of a botnet army.

I joined the conference bridge and began triaging the information. Even with limited access, the help desk had found a number of concerns. The name servers, responsible for Domain Name Service (DNS) lookups, were producing high-volume alerts and showed an abnormal number of sub-domains related to seafood. As the servers struggled to keep up, legitimate lookups were being dropped—preventing access to the majority of the internet. While this explained the "slow network" issues, it raised much more concerning questions. From where were all these unusual DNS lookups coming from? And why were there so many of them? Were students suddenly interested in seafood dinners? Unlikely. Suspecting the worst, I put on a pot of coffee and got to work.

Response and investigation.

Now that I had a handle on the incident in general, I reached out to the Verizon RISK Team, which we had on retainer, and began the process of escalating the issue. At their request, I gathered up network and firewall logs and passed them along for review. My IT security manager assured me that review would begin immediately and listed off a few of the triage steps he would be taking. All logs would be processed for known indicators of malicious activity and firewall logs in particular would be used to identify the sources of these requests.

Within hours, I had more feedback than I could handle and began the review process. The firewall analysis identified over 5,000 discrete systems making hundreds of DNS lookups every 15 minutes. Of these, nearly all systems were found to be living on the segment of the network dedicated to our IoT infrastructure. With a massive campus to monitor and manage, everything from light bulbs to vending machines had been connected to the network for ease of management and improved efficiencies. While these IoT systems were supposed to be isolated from the rest of the network, it was clear that they were all configured to use DNS servers in a different subnet.

> “The firewall analysis identified over 5,000 discrete systems making hundreds of DNS lookups every 15 minutes.

The RISK Team had provided me with a report detailing known indicators found in the firewall and DNS logs that I had sent over earlier. Of the thousands of domains requested, only 15 distinct IP addresses were returned. Four of these IP addresses and close to 100 of the domains appeared in recent indicator lists for an emergent IoT botnet. This botnet spread from device to device by brute forcing default and weak passwords. Once the password was known, the malware had full control of the device and would check in with command infrastructure for updates and change the device’s password – locking us out of the 5,000 systems.

This was a mess. Short of replacing every soda machine and lamp post, I was at a loss for how to remediate the situation. We had known repeatable processes and procedures for replacing infrastructure and application servers, but nothing for an IoT outbreak. The RISK Team was there to provide insight into how to proceed.

> “The report explained that the botnet spread from device to device by brute forcing default and weak passwords.

Luckily for me, a less drastic option existed than replacing all the IoT devices on campus. Analysis of previous malware samples had shown that the control password, used to issue commands to infected systems, was also used as the newly updated device password. These commands were typically received via Hypertext Transfer Protocol (HTTP) and in many cases did not rely on Secure Sockets Layer (SSL) to encrypt the transmissions. If this was the case for our compromise, a full packet capture device could be used to inspect the network traffic and identify the new device password. The plan was to intercept the clear text password for a compromised IoT device over the wire and then use that information to perform a password change before the next malware update. If conducted properly and quickly, we could regain control of our IoT devices.

While we waited for the full packet capture solution to be set up, I instructed the network operations team to prepare to shut down all network access for our IoT segments once we had intercepted the malware password. Short lived as it was, the impact from severing all of our IoT devices from the internet during that brief period of time was noticeable across the campus—and we were determined never to have a repeat incident.

Key lessons learned.

With the packet capture device operational, it was only a matter of hours before we had a complete listing of new passwords assigned to devices. With these passwords, one of our developers was able to write a script, which allowed us to log in, update the password, and remove the infection across all devices at once. The whole process took a matter of minutes and I made a mental note to save that script for later–although I prayed that we would never need it again. Now that the incident had been contained, we looked towards ways to prevent it from happening again.

Mitigation

- Don't keep all your eggs in one basket; create separate network zones for IoT systems; air-gap them from other critical networks where possible.
- Don't allow direct ingress or egress connectivity to the internet; don't forget the importance of an in-line proxy or content-filtering system.
- Change default credentials on devices; use strong and unique passwords for device accounts and Wi-Fi networks.
- Regularly monitor events and logs; hunt for threats at endpoints, as well as at the network level; scan for open remote access protocols on your network and disable commonly unused and unsecured features and services (such as, UPnP, RTSP) that aren't required.
- Include IoT devices in IT asset inventory; regularly check manufacturer websites for firmware updates.

Response

- Develop and follow your pre-designed IR playbooks to tackle IoT device-related incidents.
- Scope and contain incidents immediately; segregate affected subnet and restrict network ingress and egress communication to/from affected subnet.
- Change admin or console passwords of the IoT systems and controllers.
- Leverage network forensics, to include network logs, NetFlow data and packet captures.
- Consider informing law enforcement and regional CERT organizations as egress communication may have impacted other entities and the related threat intelligence could help other potential victims.

“ Don't keep all your eggs in one basket; create separate network zones for IoT systems; air-gap them from other critical networks where possible.

The evolution of the IoT.

Like any typical Gen-X technology, the IoT continues to evolve and has gone through a growth spurt over the past few years. This rapid proliferation has led to as many new issues as the underlying devices were intended to solve.

The underlying problem is that many IoT manufacturers are primarily designing their devices for functionality; and proper security testing often takes a back seat. It's even more necessary with IoT devices that the buyer scrutinizes the security of any devices they use. IoT botnets spread quickly because they don't face some of the problems conventional botnets do, due to the fact that IoT devices are often rarely patched or updated.

> "In a number of these circumstances, the IoT environment leveraged in an attack is not actually the intended victim.

In addition, the vendors that create IoT devices, along with the users that own and operate them, aren't always directly impacted by a compromise or even immediately aware that their devices played a role in a cyber-security incident. In a number of these circumstances, the IoT environment leveraged in an attack is not actually the intended victim, but rather an involuntary accomplice that is being used to attack an unrelated third-party target.

IoT threats go well beyond a typical security breach where concerns revolve around the theft of confidential data. In this new age of IoT breaches, we are seeing a growing and wide-ranging impact on our physical world as well as human life/safety (e.g. transportation or medical device incidents) and even a changing financial and legal liability landscape.

> "Organizations must think about IoT threat modeling in a manner that incorporates security and privacy by design.

Today, the IoT is not confined within an organization's typical control boundary, as the connected infrastructure has moved far beyond those control lines. These devices exist virtually everywhere, are available anytime and are on a variety of platforms. This must prompt organizations to think about IoT threat modeling in a manner that incorporates security and privacy by design.

To learn more about protecting your business, read our Data Breach Digest updates.

Find out more ›

These scenarios draw from real-world cybersecurity incident investigations. To protect victim anonymity, we modified certain details and took some creative license in writing the scenario narratives. This included, but wasn't limited to, changing names, geographic locations, and other details, such as the quantity of records stolen, and monetary loss details

VerizonEnterprise.com