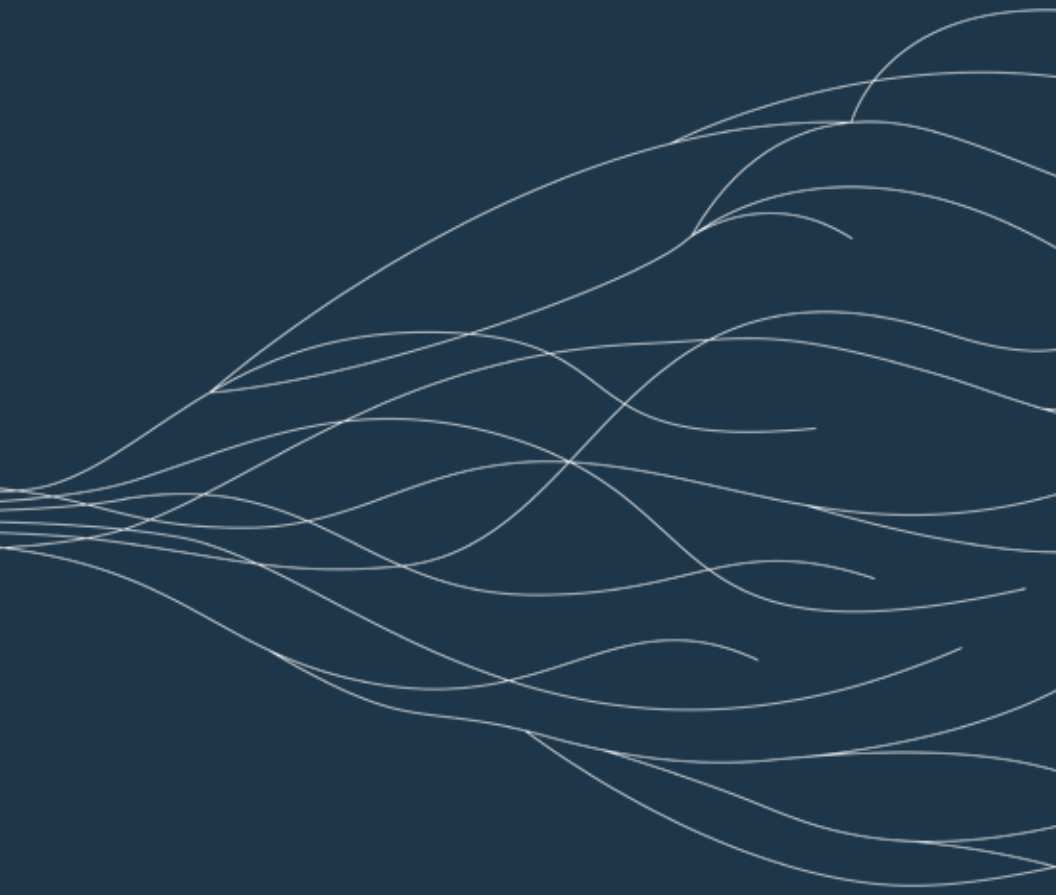


IBM Security

The weaponization of IoT devices

Rise of the thingbots

IBM X-Force® Research

IBM

Click here to start ►

Contents

Executive overview

Threat actors use botnets—networks of infected computers—for various cybercriminal purposes, most significantly distributed denial of service attacks against predefined targets. Today, botnets with distributed denial of services (DDoS) capabilities are even for sale on the Dark Web. In March 2016 our IBM report The inside story on botnets explored the botnet cybercrime landscape. How has this threat evolved?

One of the most important changes, the rising use of compromised Internet of Things devices in botnet operations, is the focus of this report. The IBM® X-Force® team has been tracking the threat from weaponized IoT devices—thingbots—and in this report we examine several 2016 attacks and the motivations behind them. Most notably, we report on the use of the Mirai botnet in several attacks and our observation of increased scanning on specific ports associated with the Mirai botnet. We also look at recent examples of attackers compromising IoT devices for malicious purposes other than botnet DDoS attacks.

The proliferation of IoT devices will continue and accelerate substantially—they are expected to account for more than two-thirds of the 34 billion internet-connected devices projected by 2020[1]—so it is vital that organizations and consumers look to implement IoT security best practices.

About this report

This IBM X-Force Research report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources, including event data, activity and trends sourced from endpoints managed and monitored by IBM.

Contents

A short history of DDoS attacks

To fully understand the current IoT botnet threat, it helps to reflect on the evolution of DDoS attacks (see Figure 1). In some ways, denial of service (DoS) attacks have changed little over time. The most significant disrupter remains the volumetric attack, in which attackers overwhelm their targets' servers by sending them more traffic than they can handle, and the aim also remains the same: preventing legitimate traffic from reaching its destination.

Back when Internet Relay Chat (IRC) was more prevalent[2] and EFnet, the modern-day descendant of the original IRC network[3], was like the Wild West, networks of Eggdrop bots[4] were a common form of DoS attack. In today's world—where we often see large numbers of compromised clients widely dispersed geographically—we wouldn't call Eggdrop bots truly "distributed," but they were an early portent of what was to come. Unlike the modern zombie clients in a botnet, Eggdrop bots intentionally created processes for controlling IRC channels, but they could also be used for DoS attacks.

Then came the era of zombie PC clients, infected by malware and controlled by "bot herders" using command and control (C&C or C2) systems. The infected clients connect to a C&C server and await instructions, either for executing in DoS attacks or for other purposes like launching massive spam campaigns.

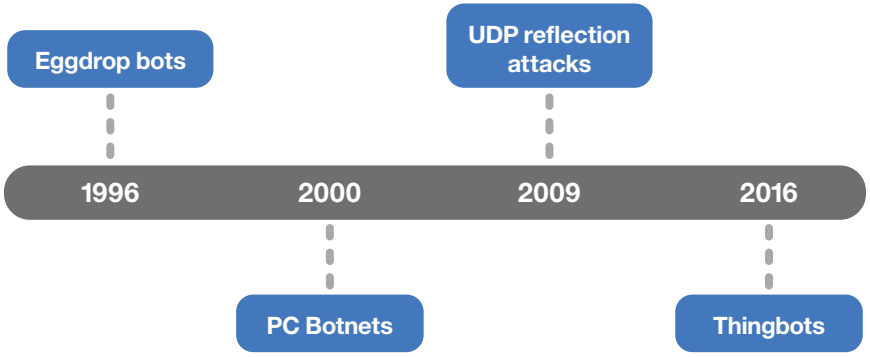
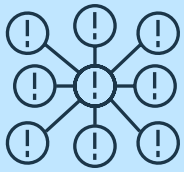


Figure 1. Attackers have evolved from exploiting PCs to exploiting IoT devices to launch DDoS attacks. Dates are approximate.

Contents

Soon, large-scale User Datagram Protocol (UDP) reflection attacks became widespread. They suited attackers because of their asymmetric nature; attackers could use a small amount of their own bandwidth to generate the attack while targeting their victims' servers with high volumes of traffic. Probably the best-known reflection vectors are Domain Name Server (DNS) amplification and Network Time Protocol (NTP) amplification attacks. Reflection attacks have been used by criminal groups such as DD4BC[5] and the Armada Collective[6] to carry out DDoS extortion schemes. The IBM report Extortion by distributed denial of service attack goes more deeply into detail on these types of attacks.

In recent years, transforming relatively easily exploitable IoT devices into thingbots has become increasingly popular. Thingbot nets appear to offer attackers a cost-effective DDoS attack option, and the attacks can be difficult to mitigate. As we can see, history does indeed have a way of repeating itself.



Botnets have evolved from networks of compromised PCs to networks of comprised IoT devices capable of launching massive DDoS attacks.

Contents

Increasing magnitude of thingbot attacks

The IBM X-Force team has been tracking the threat from weaponized IoT devices.[7] One of the first notable IoT botnet DDoS attacks, which utilized the LizardStresser DDoS tool, occurred in June 2016.[8] The attacks peaked at around 400 gigabits per second (Gbps), which is on the high side compared to previously recorded DDoS attacks that usually relied on UDP reflection attacks. The botnet, composed mainly of compromised webcams or CCTV cameras, targeted gaming sites worldwide, Brazilian ISPs, and financial and government institutions.[9]

In the months following the LizardStresser attacks the threat from thingbots grew substantially. Figure 2 shows the increase in the size in Gbps of DDoS attacks that used compromised IoT devices in whole or in part. Note the approximately 200 percent size increase over the five-month period.

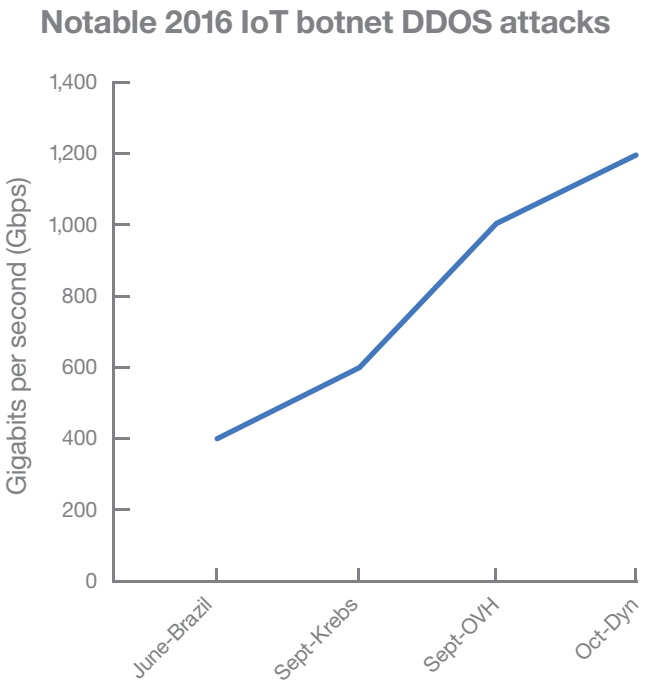


Figure 2. Size of four DDOS attacks that took place over a five-month period in 2016. Sources: Brazil, Krebs, OVH, Dyn.

Contents

In September 2016, two attacks demonstrated the increasing capabilities of IoT botnets. The first, targeting a popular security news site, began around September 20, 2016, continued for several days—longer than a DDoS attack generally lasts—and was reported by Akami Technologies, Inc. to exceed 620 Gbps.[10] A major participant was a botnet called "Kaiten"[11], more commonly known as Mirai[12], previously reported by Akamai as being used in attacks in June 2016.[13]

Just one day after the security news site attack, the founder and CTO of a cloud hosting provider reported even larger attacks. The image included in his Tweet showed two data lines from two concurrent attacks that, combined, were almost 1 Tbps. A later Tweet noted that the botnet involved was composed of some 145,607 camera and DVR devices connected through links with capacities ranging from 1 to 30 Mbps, and was able to send more than 1.5 Tbps of DDoS traffic.[14]

In October 2016, a DNS hosting provider was the victim of a possibly record-setting DDoS attack at 1.2 Tbps,[15] with major sites reportedly affected including AirBnB, Amazon, CNN, Etsy, Github, HBO, Netflix, NY Times, PayPal, Reddit, SoundCloud, Spotify, Twitter and Vox. According to a statement from Dyn, the attacks came in three waves[16]—the first around 7 AM ET on October 21, the second at approximately 12 PM ET, and the third sometime later—but they did not impact service availability. Normal services were restored around 1 PM ET the same day.

Dyn describes the attack as involving millions of IP addresses consisting of "up to 100,000 malicious endpoints"[17] with at least some attack traffic coming from a Mirai botnet. Mirai's source code was made publicly available in late September 2016 along with instructions on how to set up the entire system, so even lower-skilled attackers now have the ability to establish dangerous botnets of thingbots. An IBM X-Force Exchange collection contains relevant information regarding the attack, including indicators of compromise (IOCs).

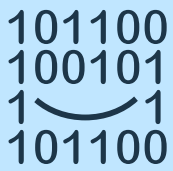
Contents

Motivations for the attacks

Determining the motivation behind an attack is often complicated by not knowing who the operators are. Brian Krebs, the man behind the "Krebs on Security" blog, speculated[18] that the motivation for the October 2016 attack on his site may have been retribution for his publishing information on the operators of a for-hire DDoS service. Krebs believes he has identified the person behind "Anna Senpai," the name under which the Mirai botnet source code was released, along with the identity of one other co-conspirator. He has written an article on his investigation[19] that's an intriguing read.

The motivation for the October 2016 attack on the DNS hosting provider Dyn is unclear. There have been reports[20] of a group named New World Hackers claiming responsibility, but another comment made in a Tweet[21] from WikiLeaks appears to infer that the attack was carried out by WikiLeaks supporters in retribution for Julian Assange having his internet access cut off, while a third report[22] suggests that the attack was carried out by "script kiddies" who congregate on an online forum dedicated to hacking topics. It's reported that the forum[23] has now discontinued its section allowing ads for DDoS-for-hire services. So take your pick. Since no solid attribution could be made, any of the options could have been the real reason behind the attack.

IBM X-Force has not observed a stated reason for the aforementioned attack on the cloud hosting provider. For further reading on the motivations of attackers, we recommend the IBM report Know your enemy: Understanding the motivation behind cyberattacks.



The reasons behind DDoS attacks can range from malice and revenge to "script kiddies" who perpetrate attacks for the fun of doing it.

Contents

Mirai botnet scanning activity: Ports 23, 2323 and 7547

The IBM X-Force Threat Analysis Service includes port metrics obtained through a darknet, a block of IP addresses that under normal circumstances should not receive any connection requests. However, these IP addresses will generally not be excluded from IP address scanning. And scans such as those generated by the Mirai botnet will often simply cycle sequentially through the total range of IP addresses, although most scans will avoid the private address spaces defined in RFC1918[24] (i.e. 192.168.0.0 - 192.168.255.255) from the Internet Engineering Task Force (IETF[25]).

In May 2016, IBM Security blogged about how one of the oldest protocols for accessing remote computers, Telnet, could be an attacker's gateway to gain unauthorized access into IoT devices.[26] Looking at the graphs from our port metrics, we see that on September 13, 2016, port 2323 (TCP), an alternate port for Telnet, began showing up in our top five most-scanned ports. Port 23 (TCP), the standard port for Telnet, often shows up in the top five. Both ports are associated with the Mirai botnet, which scans them looking for vulnerable IoT devices (see Figure 3).

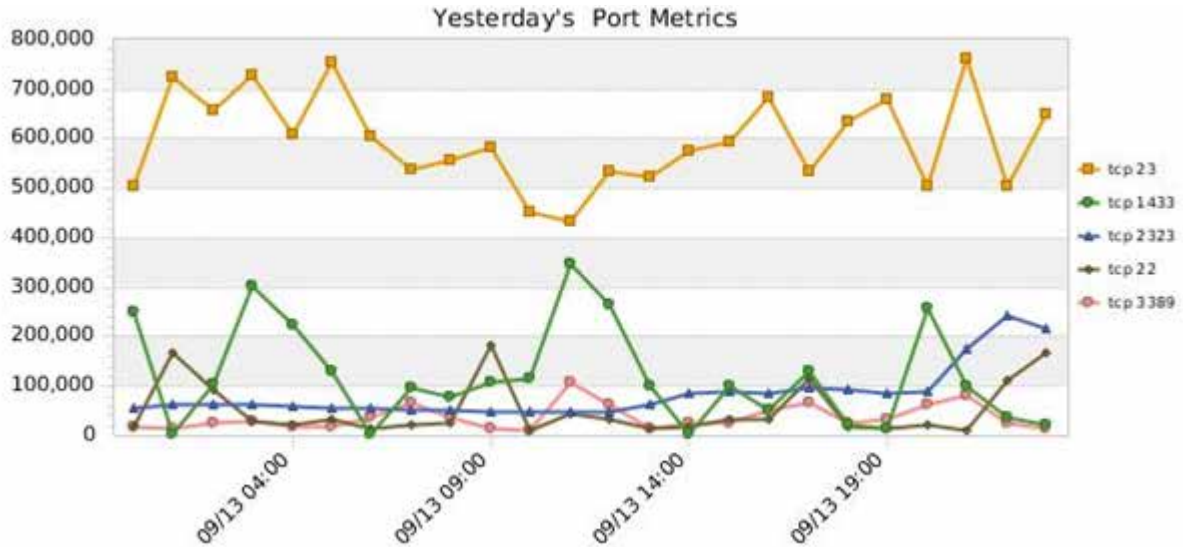


Figure 3. IBM X-Force Threat Analysis Service Port Metrics, September 13, 2016. The value of the Y-axis is the number of connection attempts.

Contents

While the volume of connection requests varied day to day, TCP ports 23 and 2323 were the top two ports the day before the Dyn attack (see Figure 4).

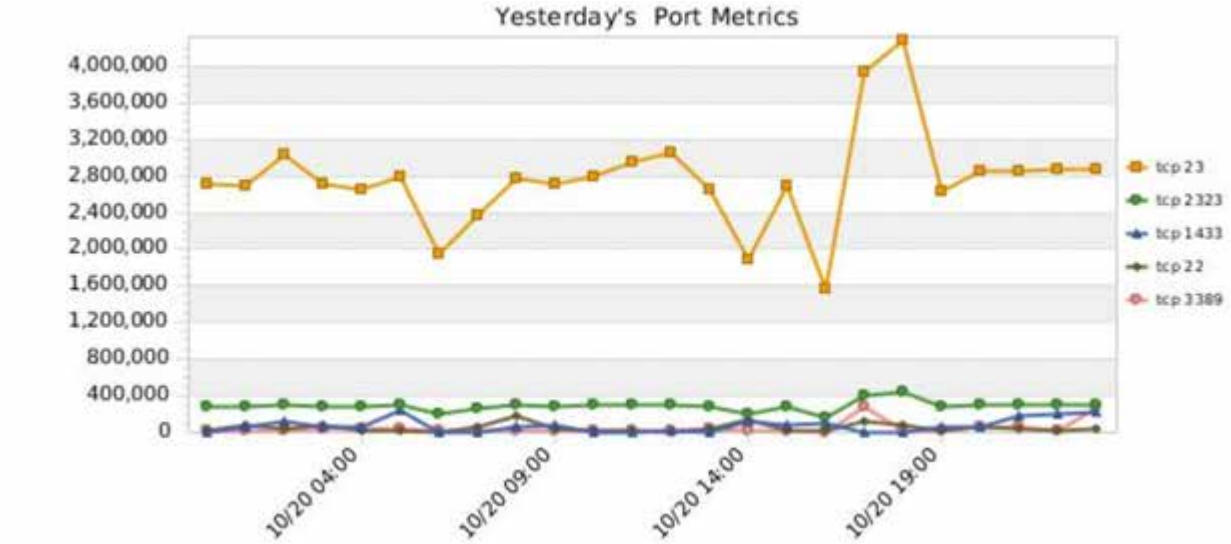


Figure 4. IBM X-Force Threat Analysis Service Port Metrics, October 20, 2016. The value of the Y-axis is the number of connection attempts.

Contents

The Mirai code was modified to include exploitation of another vulnerability, TR-069[27], and used TCP port 7547.[28] That port started showing in our top-five port metric chart in mid-November and by November 27 was second only to Telnet (see Figure 5).

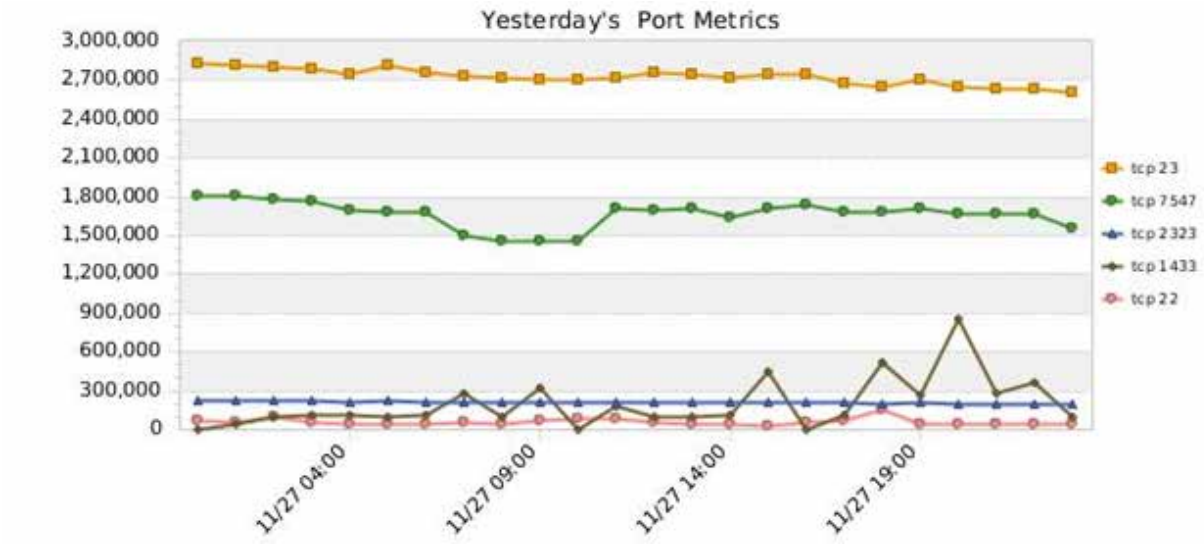


Figure 5. IBM X-Force Threat Analysis Service Port Metrics, November 27, 2016. The value of the Y-axis is the number of connection attempts.

This was followed by reports of attacks on the customers of ISPs who were providing their users with equipment that suffered from the TR-069 vulnerability. Deutsche Telekom, for example, reported that around 900,000[29] of its users were affected by Mirai botnet attempts to compromise devices. Another report from Incapsula shows the UK ISP experienced similar issues.[30] Perhaps the only bright spot is that the attempts to compromise end users' routers were detected and the various ISPs took steps to mitigate the issue. Other devices such as webcams and DVRs tend to go unnoticed, at least until they are used in attacks, and even then they may not be remediated by an ISP or the end user. Many users neglect to change the default passwords on these devices or re-use credentials on other sites, which exacerbates the issue. The published Mirai source code contained a list of default IoT device usernames and passwords that attackers could use in brute-force attacks to compromise their targets.[31]

At the end of January 2017 our port metrics still showed significant scans for port 23 (Telnet), and while activity on ports 2323 and 7547 was still occurring, the volume was lower (see Figure 6).

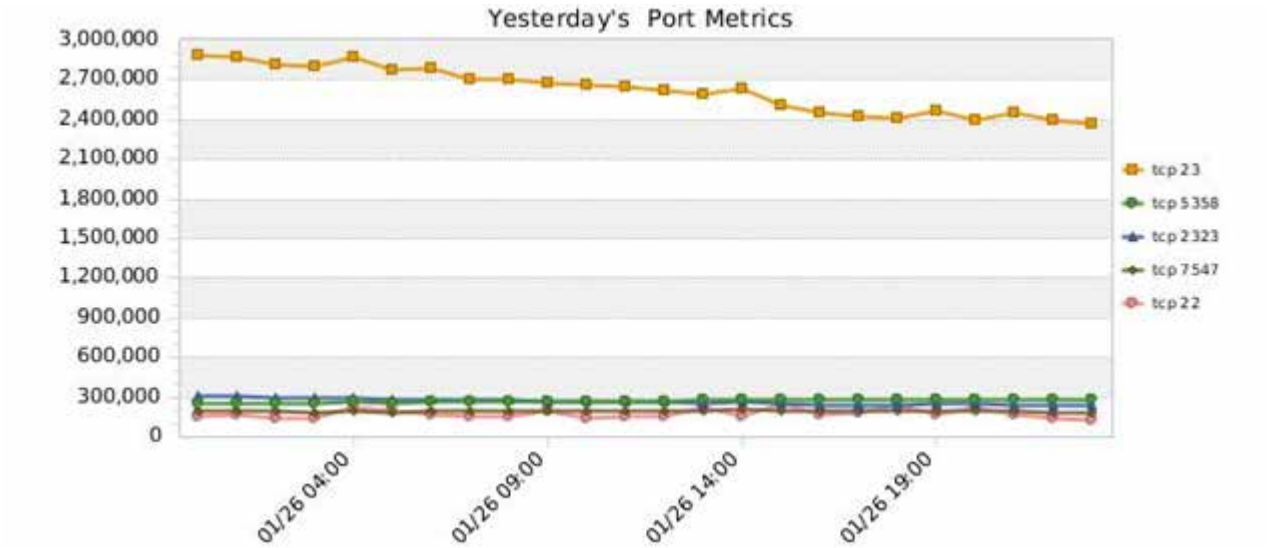


Figure 6. IBM X-Force Threat Analysis Service Port Metrics, January 26, 2017. The value of the Y-axis is the number of connection attempts.

Contents

And new twists

In February 2017, Trend Micro reported new twists in how the Mirai botnet is attempting to increase its size.[32] The original Mirai malware targets IoT devices running Linux-based firmware. A new Windows Trojan has been discovered that connects with C&C servers on infection and obtains a list of IP addresses to scan for exploitation. If a Linux-based system is successfully compromised by the Trojan, an instance of the Mirai botnet code is installed to create a new bot. If the victim system is a Windows machine, however, a copy of the Trojan itself is installed which in turn will contact the C&C servers for more IP addresses to scan. Trend Micro believes this approach "drastically increases [the Mirai bot's] distribution capabilities."

In March 2017, Incapsula reported that one of their customers, a US college, suffered a massive DDoS attack that lasted more than two days. According to the report, the analysts believed that a new version of the Mirai malware was used, 'modified to launch more elaborate application layer attacks.' Interestingly, DVRs manufactured by the same vendor made up 56 percent of all IPs used in the attack.

It's not only Mirai exploiting IoT devices

Other actors and campaigns have also focused on IoT devices. In one reported example, attackers attempted to exploit Brazilian home routers that still had the default username/password combinations set by the provider.[33] This exploitation can be accomplished using JavaScript and attacks such as Cross-Site Request Forgery (CSRF). Victims redirected to a malicious webpage may find themselves running JavaScript in their browser. The script tries to locate the router at default local addresses, gain access using default credentials and, when successful, execute commands. Reportedly, compromised systems in this case appear to be used for phishing schemes through modifying DNS settings. This type of attack is not new, and there are many other examples[34] of compromised IoT devices being used to hijack a user's DNS settings and redirect the victims to sites under the control of an attacker.

Contents

Another notable incident occurred in Washington DC in the week prior to the US presidential inauguration. Reportedly, 123 of 187 network video recorders used to record the data from DC police surveillance cameras were compromised by one of two types of ransomware.[35] Knowing that the Mirai botnet and others have successfully targeted DVRs in the past, we wonder whether we're seeing a harbinger of IoT ransomware attacks to come.

All of these examples point out that the Internet is a hostile environment populated by cybercriminals who, if not prepared for through design, implementation, testing and response, will identify and exploit weaknesses in any connected equipment. Whether it's a computer, mobile device or household appliance, by being connected to the internet it could become subject to attack. The attacks also point out that the effects of the attacks and the costs to those affected could be completely separate and removed from the intended use of the device or equipment itself. The ability to insert or change the instructions running in such devices leaves open the possibility of ransomware-style attacks against equipment that controls physical systems or attacks that can endanger humans or the environment by changing the equipment's behavior or actions.

If a device is connected to the internet—a camera, video recorder, computer, mobile device, router or household appliance—it is subject to attack.

Contents

Developing standards and guidelines

Late in 2016 we saw reports that the European Commission[36] and US lawmakers[37] were considering issues regarding the security of IoT devices. Enacting effective legislation will be challenging, however, because laws are national or regional in nature, while cybercriminals act globally, making law enforcement difficult. There are many additional difficulties lawmakers face in terms of legislating standards for IoT devices. One challenge involves developing a clear, legally enforceable definition of what constitutes an IoT device. Furthermore, any legislation is unlikely to have an immediate effect because of the time it would take for manufacturers to adopt new security standards and practices for IoT devices. At the same time, rapid innovation makes it difficult or impossible for regulations to adequately keep pace.

Legal murkiness has risen in the wake of a lack of clear guidelines. For instance, one complaint filed by the US Federal Trade Commission (FTC) against a vendor that produces IoT devices alleges that the vendor has "failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access."[38]

The good news for IoT device and solution providers is that there are several industry consortia and groups worldwide, including the Industrial Internet Consortium (IIC), IoT Security Foundation, National Institute of Standards and Technology (NIST)[39], and the Alliance for Internet of Things Innovation (AIOTI)[40], that are developing IoT frameworks, guidelines and recommendations.

Contents

What are the takeaways from these attacks?

The first takeaway is that as long as easily exploited IoT devices remain connected directly to the Internet and remotely accessible from it, bad actors will continue to weaponize them.

There has been significant growth in the magnitude and complexity of thingbot-based attacks throughout 2016. The release of the Mirai source code probably means that more bad actors will be attempting to create their own IoT botnets. Some may try to further develop the code, for example adding the ability to target a greater range of IoT devices. Attackers don't even need to create their own code. They can purchase access to DDoS systems usually referred to as "Stresser" or "Booter" services. One ad on the AlphaBay Dark Web site claimed to offer access to a botnet capable of delivering 1 Tbps of traffic for $7,500 per 100K bots.[41] The Tb stands for Terabits, of course, but in this context it could easily mean Terror-bits!

Mirai is not the only IoT botnet out there. Other well-known examples include BASHLITE[42] and what appears to be a newer entrant, Hajime[43]. We have seen reports that the BASHLITE malware family alone may have compromised up to a million IoT devices.[44] Another new entrant, though in some ways derivative from previous code, is Linux/IRCTelnet. It uses Telnet to locate and compromise vulnerable devices and IRC servers for command and control. Reportedly it took only five days to establish a botnet of some 3,500 devices.[45]

While this report has focused on just a few very notable attacks, the fact is that thingbots are being used in many other attacks such as those carried out against gaming sites. We think the problem of easily compromised IoT devices is likely to get worse before it gets better.

Contents

How to prevent your IoT device from becoming part of a massive botnet

Like other attack surfaces such as web servers and databases, IoT devices require hardening as soon as they are installed to mitigate the threat of compromise. Endpoint security solutions can help lock down these devices before cybercriminals attack.

Home and enterprise users should:

- Carefully read the device's instructions or contact the manufacturer for support
- Secure home networks and locate IoT devices on the secured networks
- Change all default passwords and user IDs
- Audit devices to determine which ones have default accounts
- Opt for devices made by manufacturers with a track record of security awareness
- Utilize firmware/software updates made available by IoT device providers
- Disable the universal plug-and-play protocol on any routers

Enterprise security teams should:

- Isolate IoT devices on protected networks
- Perform security testing of IoT devices
- Create an asset inventory that includes mapping the network to discover all paths of ingress and egress; this could allow you to discover that the IoT network has its own internet gateway that is not enterprise-class and does not conform to security policies or applicable laws, regulations and contracts
- Monitor network access to determine normal behaviour and detect anomalies
- Apply access controls between IoT devices and IT resources using enterprise firewalls, intrusion prevention systems, and integration with identity and access management, to the extent that it is supported
- Collaborate with the Internet of Things Security Foundation (IoTSF) to help secure IoT technologies
- Utilize recommendations and capabilities suggested by NIST and the Industrial Internet Consortium (IIC) Security Framework,[46] including:
  - NIST 800-57 - Key Management (all parts, but especially Part 1 - now in Rev. 4)
  - NIST Cybersecurity Framework (for critical infrastructure) - updated most recently in January 2017 - https://www.nist.gov/cyberframework
  - NIST 800-160 - Systems Security Engineering
  - NIST 1800-7 - a recently published cybersecurity practice guide for Electric Utilities (has to do with monitoring)
  - NISTIR 8063 - Primitives and Elements for IoT
  - NIST SP-800-131 and FIPS-140 where applicable—i.e. using validated crypto
  - NIST SP-800-171 / ISO20243

Device manufacturers and operators are encouraged to review IoT Security: An IBM position paper for recommendations.

Contents

The bottom line

DDoS attacks have evolved over time. The weaponization of IoT devices into attacking DDoS botnets is simply the latest trend, the current "thing" from which to create an army of bots. There are several drivers underlying a majority of issues with IoT devices. And as DDoS attacks have become more potent and more common we have witnessed a parallel proliferation of DDoS mitigation services, to the point where it might not be inaccurate to describe the current situation as something of an arms race. Thingbots are only the current chapter in the story. The bad guys will continue to seek out ways to asymmetrically attack their victims. As DDoS mitigation companies improve their ability to handle and defend against even larger attacks, the attackers will be seeking ways to overwhelm the defenses. It would be nice to think that this was the final chapter, but it seems rather unlikely. A more instrumented, connected and cognitive world is here. Attention to security, from the smallest to the largest of these connected devices, is just as important as securing computers, cloud systems, laptops and mobile devices.

Manage the threats that come with the benefits of IoT

The Internet of Things provides both businesses and individuals with unparalleled amounts of meaningful data. Yet with this access comes the potential for security compromises. IBM IoT security experts can help. The IBM Watson IoT™ Platform, which provides a comprehensive solution to address the complexity of IoT security, has security by design engineered into the platform and the infrastructure upon which the platform is based.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,500 security patents.

Contents

About the author

Lyndon Sutherland, Senior Threat and Intelligence Analyst, IBM X-Force, has been involved in network engineering and security for more than twenty years, fourteen of which have been with IBM. His work with IBM as a researcher and analyst led him to joining the IBM X-Force Threat Analysis Service in 2008. He also works with the Managed Security Services Threat Research Group writing and contributing to research papers.

Contributors

Timothy J. Hahn—IBM Distinguished Engineer and Chief Architect, Internet of Things
Michelle Alvarez—Threat Researcher and Editor, IBM Managed Security Services

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

For more information on security services, visit: **ibm.com**/security/services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

Contents

References

[1] http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10

[2] https://en.wikipedia.org/wiki/Internet_Relay_Chat

[3] https://en.wikipedia.org/wiki/EFnet

[4] https://www.eggheads.org/

[5] https://securityintelligence.com/ddos-extortion-ransomwares-older-cousin/

[6] https://securityintelligence.com/pay-us-the-money-or-the-website-gets-it-extortion-by-ddos/

[7] https://securityintelligence.com/the-threat-from-weaponized-iot-devices-its-bigger-than-you-think/

[8] http://www.zdnet.com/article/lizardstresser-botnet-targets-iot-devices-to-launch-400gbps-attacks/

[9] https://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser/

[10] https://blogs.akamai.com/2016/10/620-gbps-attack-post-mortem.html

[11] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/kaiten-std-router-ddos-malware-threat-advisory.pdf

[12] https://st.drweb.com/static/new-www/news/2016/september/Investigation_of_Linux.Mirai_Trojan_family_en.pdf

[13] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/kaiten-std-router-ddos-malware-threat-advisory.pdf

[14] https://twitter.com/olesovhcom/status/779297257199964160

[15] https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/

[16] http://hub.dyn.com/static/hub.dyn.com/dyn-blog/dyn-statement-on-10-21-2016-ddos-attack.html

[17] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[18] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[19] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

[20] http//www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145

[21] https://twitter.com/wikileaks/status/789574436219449345

[22] https://www.flashpoint-intel.com/action-analysis-mirai-botnet-attacks-dyn/

[23] https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar/

[24] https://tools.ietf.org/html/rfc1918

[25] https://www.ietf.org/about/

[26] https://securityintelligence.com/telnet-an-attackers-gateway-to-the-iot/

[27] https://en.wikipedia.org/wiki/TR-069

[28] https://securityintelligence.com/mirai-evolving-new-attack-reveals-use-of-port-7547/

[29] https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862

[30] https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.html

[31] https://securityintelligence.com/the-internet-of-trouble-securing-vulnerable-iot-devices/

[32] http://blog.trendmicro.com/trendlabs-security-intelligence/mirai-widens-distribution-new-trojan-scans-ports/

[33] http://www.welivesecurity.com/2016/10/21/cybercriminals-target-brazilian-routers-default-credentials/

[34] https://www.cert.pl/en/news/single/large-scale-dns-redirection-on-home-routers-for-financial-theft/

[35] https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html

[36] http://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/

[37] http://www.cio.co.nz/article/610267/us-lawmakers-balk-call-iot-security-regulations/

[38] https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf

[39] https://www.nist.gov/

[40] http://www.aioti.org/

[41] https://twitter.com/mikko/status/790313284863979522

[42] https://securityintelligence.com/news/bashlite-malware-uses-iot-for-ddos-attacks/

[43] https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf

[44] https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/

[45] http://blog.malwaremustdie.org/2016/10/mmd-0059-2016-linuxirctelnet-new-ddos.html

[46] http://www.iiconsortium.org/IISF.htm

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2017

SEL03128-USEN-00