Blackcomb Networks

IoT Security

May 15, 2017

Problem Statement

Retail, Commercial, and Small-Medium Businesses will see an explosion in the number of devices actively connected to the Internet. Gartner, IDC, and other analysts expect about 20-30 billion connected devices by 2020 besides smartphones, tablets, and computers [1]. While the variability of this number is high, one cannot deny the fact that that industry is not prepared to address the core security aspect of IoT devices and infrastructure. Specifically, device attack surface has and will continue to significantly increase, much beyond what traditional enterprise networks are capable to handle. Attack surface has increased because devices choose to use non-standard third-party cloud infrastructure to communicate over disparate platforms running non-standard protocols. Thus, it becomes significantly more difficult to protect IoT devices from Data Leaks, and from being targeted as victim devices to take control of networks.

Who is Vulnerable?

Recent reports [2, 9] and vulnerabilities indicate that SMB are at a risk of greater cyber attack, as is demonstrated by WannaCry ransomware. In fact, WannaCry used an SMB vulnerability patched by Microsoft (MS17–010) in March 2017 to exploit target machines in various countries [2,3].

At the same time, Gartner and SurfWatch Labs [15], and Scalar IOT market analysis [16] suggests that 8-10 billion Smart IoT devices will be connected to the Internet, 25% of which are non-PC smart embedded IOT devices. Sophos Labs 2017 report [4] identifies through their HoneyPot service that Linux-based malware are on the raise in 2016, and continuing onto 2017. These malware built to evade AV detection with static updates, encrypted strings and packet hacking techniques. These are

typically doable on embedded devices, especially considering the fact that most of devices do not carry any mechanism to identify them, use weak or default passwords, and communicate in plaintext to backend infrastructure.

What is your Stake?

Attackers gain access to devices, bricking them or making them victim of further in-network attacks. For instance, see recent BrickerBot [7] attack. Or Mirai botnet [4] that was used to hijack Internet cameras to launch coordinated attack onto Dyn.

As noted by Bruce Schneier on IoT security [13, 14], we will continue to see significant open security risks and increases, specifically due to IOT. Per Schneier [14], "To answer your question, I think we're going to entering a less secure time due to the low-cost free-wheeling world that will be the Internet of Things. It's not going to be because of cryptography problems; it'll be because of computer security and networking problems." Question was, "What changes or progress do you envision in the next decade?"

- According to HPE 2015 IOT report [10], several IOT devices continue to use HTTP raw stream without any kind of encryption e.g. passwords, username, and raw photos/videos. About 70% devices uses unencrypted network service
- Almost all of these devices use insufficient authorization/authentication such as weak or default passwords
- As per Podsnap blog [11], camcloud, Imeji [15] uses unencrypted FTP'ing of household videos/images onto their AWS servers, that could be overwritten

In addition, ISPs, and other retail/SMB-targeted middlemen use traffic analysis to attempt to find nature of transactions, and make something out of it. For instance, Comcast Business attempting to sell your web history to 3rd party could reveal significant Intellectual Property Advantages of SMBs [12].

How does Blackcomb IOT Security Solution Help?

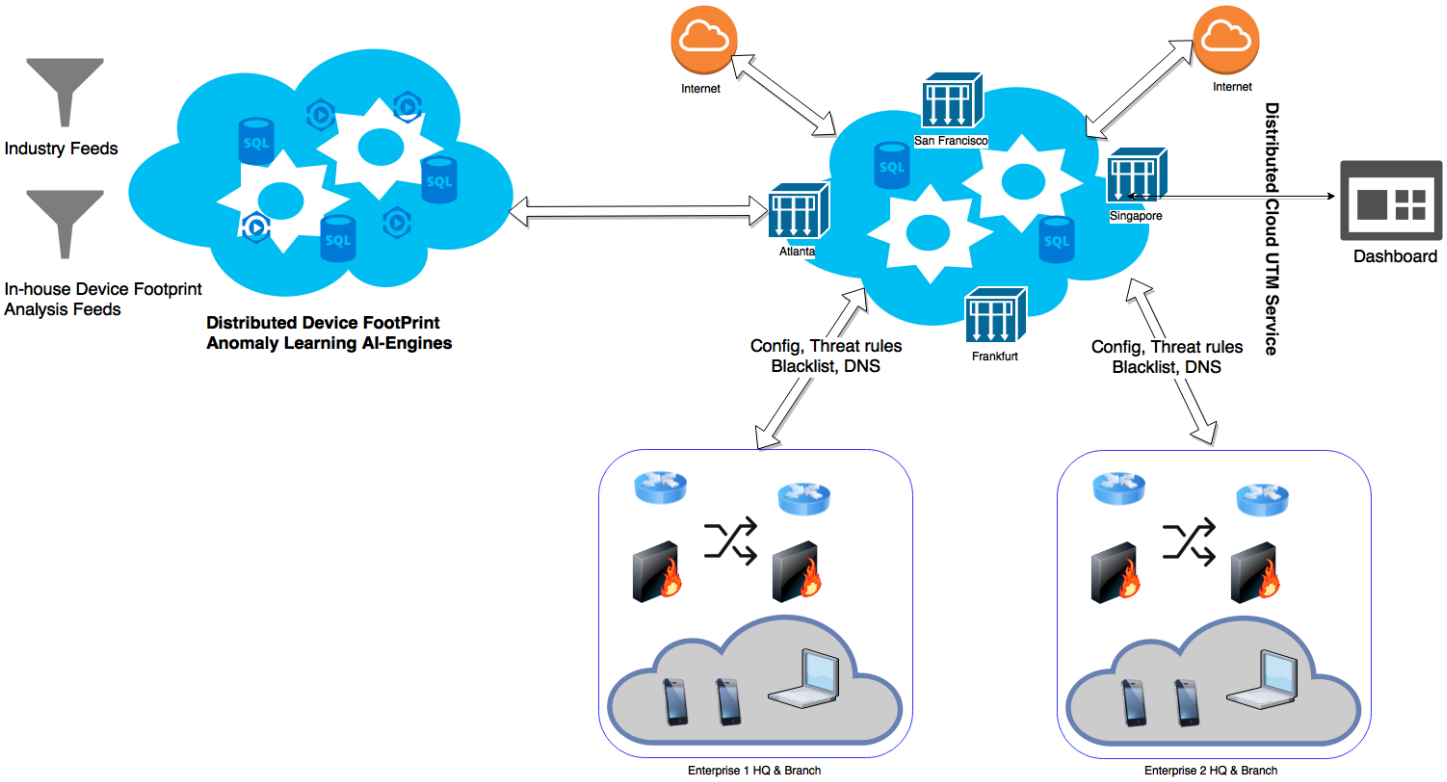
Blackcomb Networks' makes a compelling case for a convincing solution to address attack surface and attack dynamics in the following ways:

1) Global Distributed Internet gateways protecting all edge access onto Internet, enabling complete protection of all IOT devices using perimeter gateways, and enabling dual-form authentication to securely communicate with any backend vendor platform.

   Towards this, we are building a secure Cloud-based Advanced/UTM & Firewall service backend infrastructure. Backend cloud infrastructure provides secure inline traffic processing services, and enabling distribution of security/policy rules specific to companies requesting services. On-premise Firewall/UTM appliance or Virtual Appliance will support these. Both components perform inline as well as offline packet processing.

2) Unique AI-based automatic threat detection & anomaly learning engines in backend constantly "upgrading" ever-changing cyber dynamics intelligence

   We are building a massive cloud-based device-footprint infrastructure capability against individual device, their capabilities, and their platform/infrastructure, their messaging, and their communication patterns only to automatically classify known vs unknown behavior that serves as targets of suspicious activities



References

1) Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated, Aug. 2016

   http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

2) SMEs Still Too Complacent About Cyber Attack, Apr. 2017

   https://www.forbes.com/sites/davidprosser/2017/04/18/smes-still-too-complacent-about-cyber-attack/#40a360f40901

3) WannaCry — The largest ransom-ware infection in History, May 2017

   https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58

   https://blog.comae.io/the-nsa-compromised-swift-network-50ec3000b195

4) Sophos Lab 2017 Report, Feb. 2017

https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2017-malware-forecast-report.pdf?la=en

5) Cisco Cybersecurity 2017 Report, Jan. 2017

http://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

6) Dark Reading – Your IoT Baby Isn't as Beautiful as You Think It Is, May. 2017

http://www.darkreading.com/iot/your-iot-baby-isnt-as-beautiful-as-you-think-it-is-/a/d-id/1328825

7) This Hacker Is My New Hero, Apr. 2017

https://gizmodo.com/this-hacker-is-my-new-hero-1794630960

https://arstechnica.com/security/2017/04/rash-of-in-the-wild-attacks-permanently-destroys-poorly-secured-iot-devices/

8) Scalar IOT Market Research, Oct. 2016

https://www.scalarmarketresearch.com/market-reports/internet-of-things-iot-security-market

9) HPE IOT Security Report 2015

http://h20195.www2.hpe.com/V4/getpdf.aspx/4aa5-4759enw [PDF]

10) Spying on myself, Jan. 2016

http://blog.podsnap.com/amcrest.html

11) Comcast wants to sell your Web history to advertisers, Aug. 2016

https://www.washingtonpost.com/news/the-switch/wp/2016/08/03/comcast-wants-to-sell-your-web-history/

12) Schneier on why IoT security is very important, July 2016

https://www.schneier.com/blog/archives/2016/07/real-world_secu.html

13) Schneier AMA on Reditt AMA, Aug. 2016 https://redd.it/4vs90j

14) SurfWatch IoT Devices Expanding Your Digital Footprint, Mar. 2017

https://www.slideshare.net/SurfWatchLabs/iot-devices-expanding-your-digital-footprint

Contact Us

BlackComb Networks, Inc.

1159 Sonora Ct.

Sunnyvale CA 94086

info@blackcombnetworks.com

Phone: (408)442-1289

https://blackcombnetworks.com