NETSCOUT | Arbor

Devices Without Identity: Internet of Things (IoT) in the Enterprise Network

Arabella Hallawell

National Institute of Standards and Technology
U.S. Department of Commerce

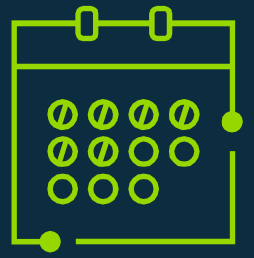
The Defender's Reality in 2017

9 Min.

The **mean time for initial compromise** of a network.

44%

44% of advanced attacks in 2016 **used social engineering or IT applications, NOT malware as entry points**



140+$^{+}$

The **average dwell time (mean time to detect)** a breach to the business.

60%

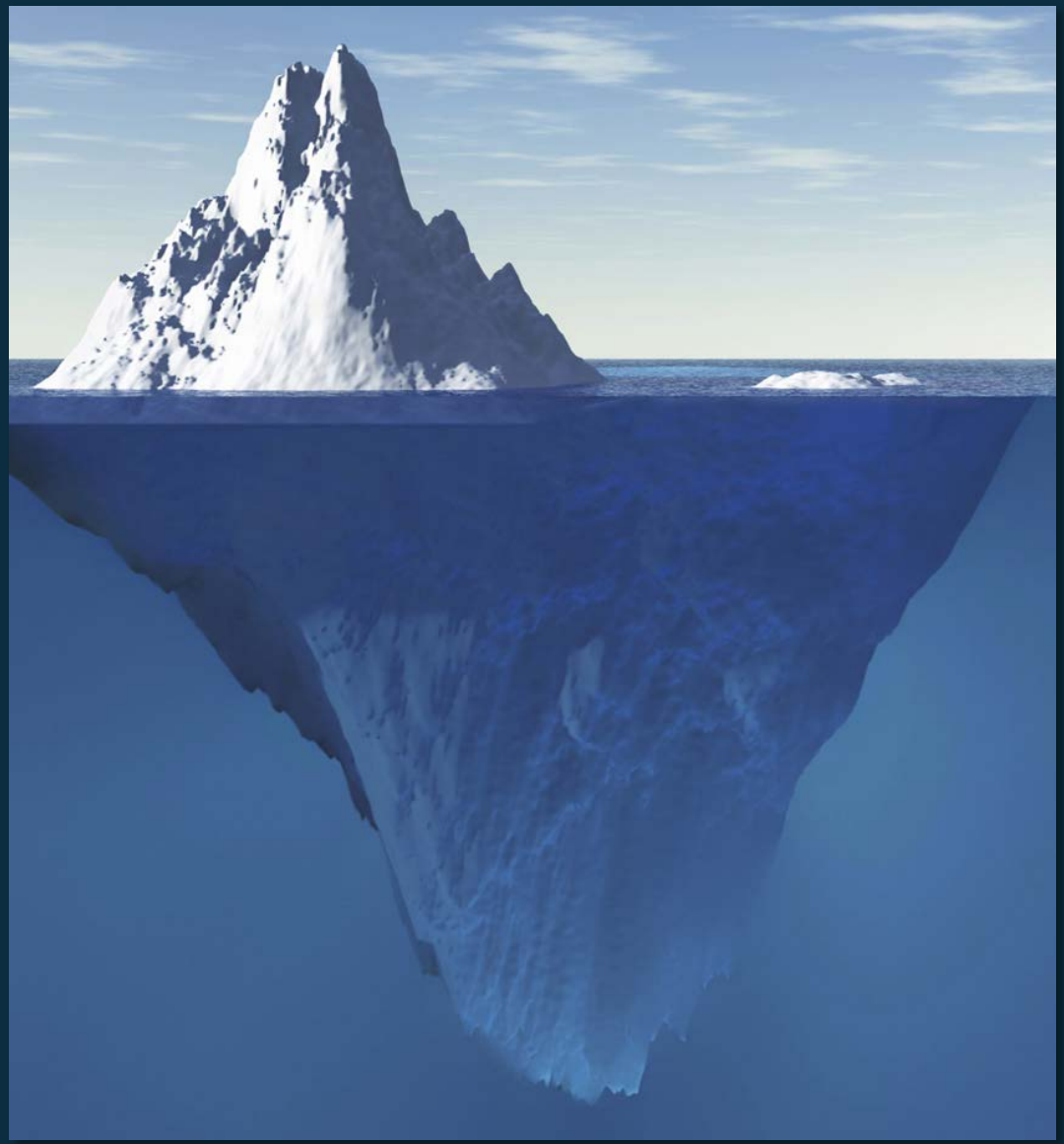
60% of enterprises **take longer than 3 days** to investigate a critical security event.

What We See Today…

- An unprotected IoT device on the Internet will get infected within 1 minute.

- An IoT device located behind a NAT device or a Firewall is not accessible from the Internet and we believe is (mostly) secure.

But this is not always the reality…



The Weakest Link IoT: Devices Without Identities

Consumer Grade Devices on Enterprise Network

Traditional Security Models Don't Apply

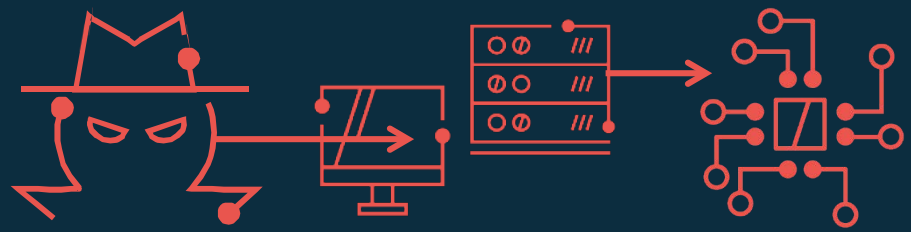
NAC Struggles to Control

Greater Attack Surface

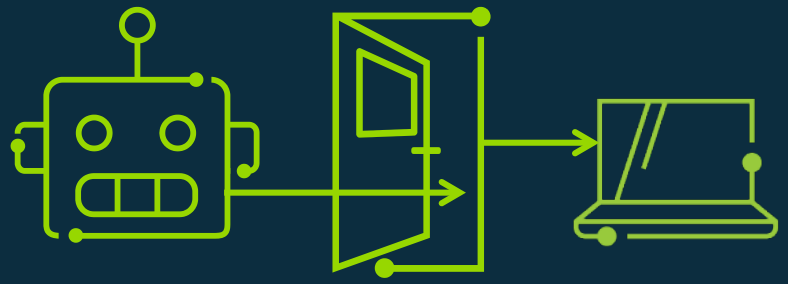
The Defender's Reality with IoT in 2017

<3 Min.

The **mean time for initial compromise** of a IoT device.



Use Malware as way to infect entire network (Windows Mirai)



Back doors for automated Botnet / DDoS.

Physical damage

Implications & Potential Consequences

- **The Zombie horde**

  A single infected Windows computer has now the capability to infect and subvert the ”innocent” IoT population into zombies, all under the control of the attacker.

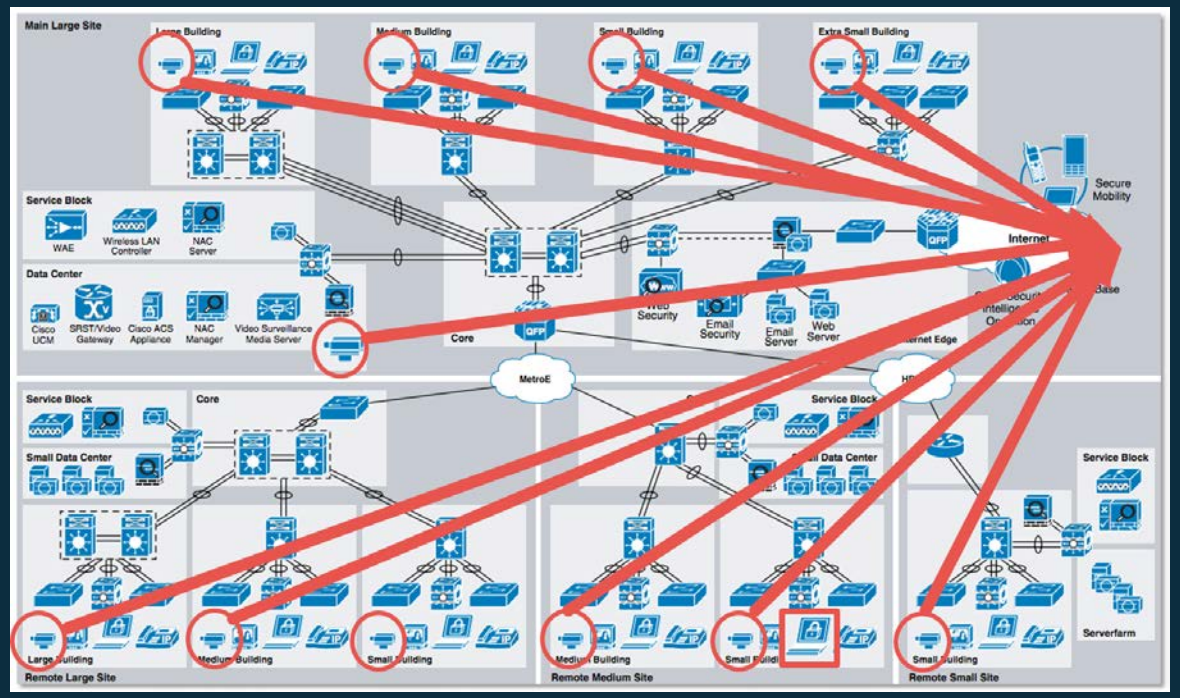
- **The attackers weapon arsenal**

  The attacker can now use the zombies to:

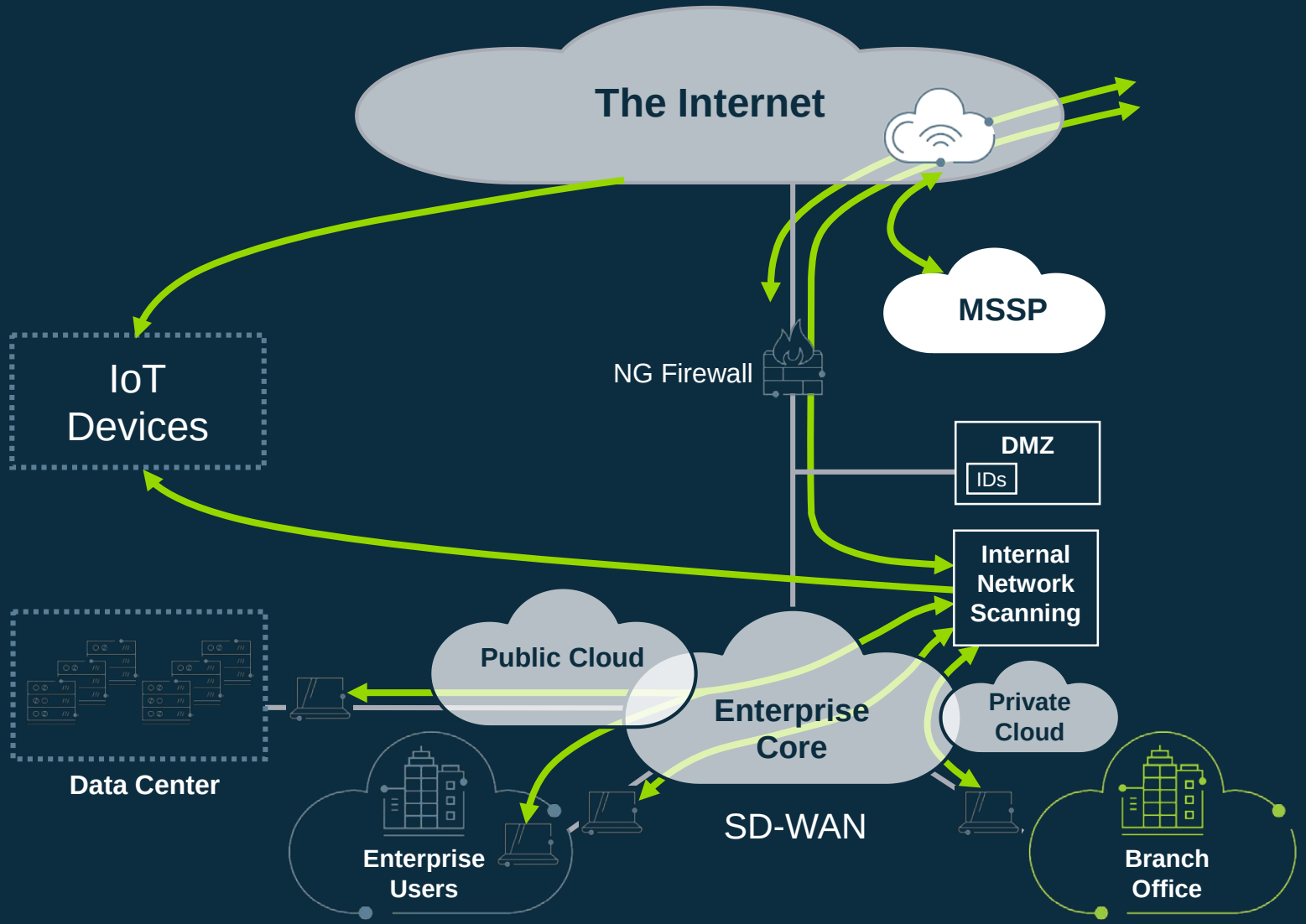
  1. Infect other IoT devices.
  2. Launch outbound attacks against external targets.
  3. Perform reconnaissance on internal networks, followed by targeted attacks against internal targets.

Launching Outbound DDoS Attacks

- Attack activity generates a lot of traffic. Mirai can for example launch:
  - UDP / ICMP / TCP packet flooding
  - Reflection attacks using UDP packets with spoofed source IP addresses
  - Application level attacks (HTTP / SIP attacks).
  - Pseudo random DNS label prefix attacks against DNS servers.
- This attack traffic will quickly fill up any internal WAN links and will also will cause havoc with any stateful device on the path, including NGFWs.

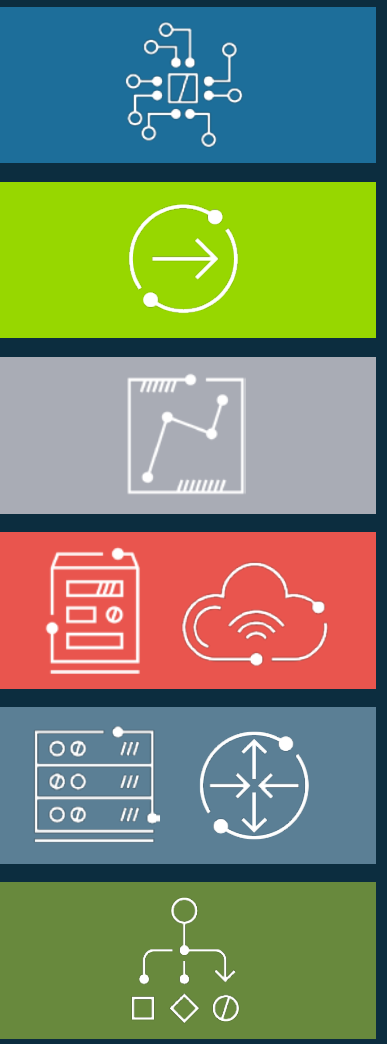


IoT: Enterprise Security Architecture Revisit



Defending Against IoT InternalThreats

- Implementing Network segmentation and harden (or isolate) vulnerable network devices and services.
- Utilizing flow telemetry to analyze external and internal traffic. This is necessary for attack **detection**, **classification** and **trace back.**
- Deploying multi-layered DDoS protection.
- Scanning for misconfigured and abusable services.
- Implementing Anti-Spoofing mechanisms on all edge devices.



Q&A / THANK YOU

Contact Information:

Arabella Hallawell, (Job Title here xxxxxxxxxxx)
ahallawell@arbor.net