Breach Readiness and Response

Luxembourg Internet Days

Philippe Roggeband
GSSO EMEAR – Manager, Business Development
15th November 2017

Organizations take, on average, 191 days to detect a breach and 66 days to contain it.

(Source: Ponemon Institute)

Readiness Response

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agenda

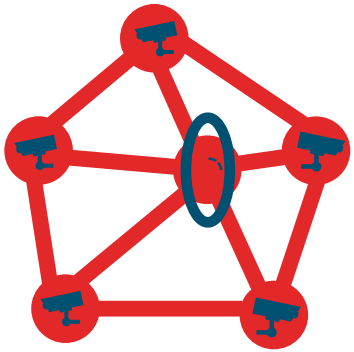
- What are we facing?
- Breach Readiness
- Breach Response
- Can we help?

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

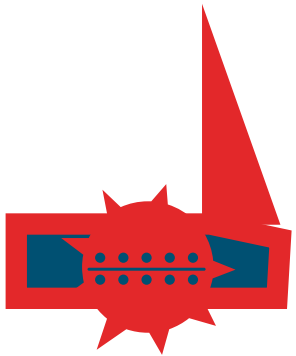
Exploit Kits Fade into the Shadows

Adversaries focus on other attacks

Exploit Kits



DDoS



Email

Ransomware

Exploit Kits

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

Emerging Ransomware Tactics

Using ransomware codebases to their advantage

Ransomware-as-a-Service (RaaS) Platforms Are Growing Fast

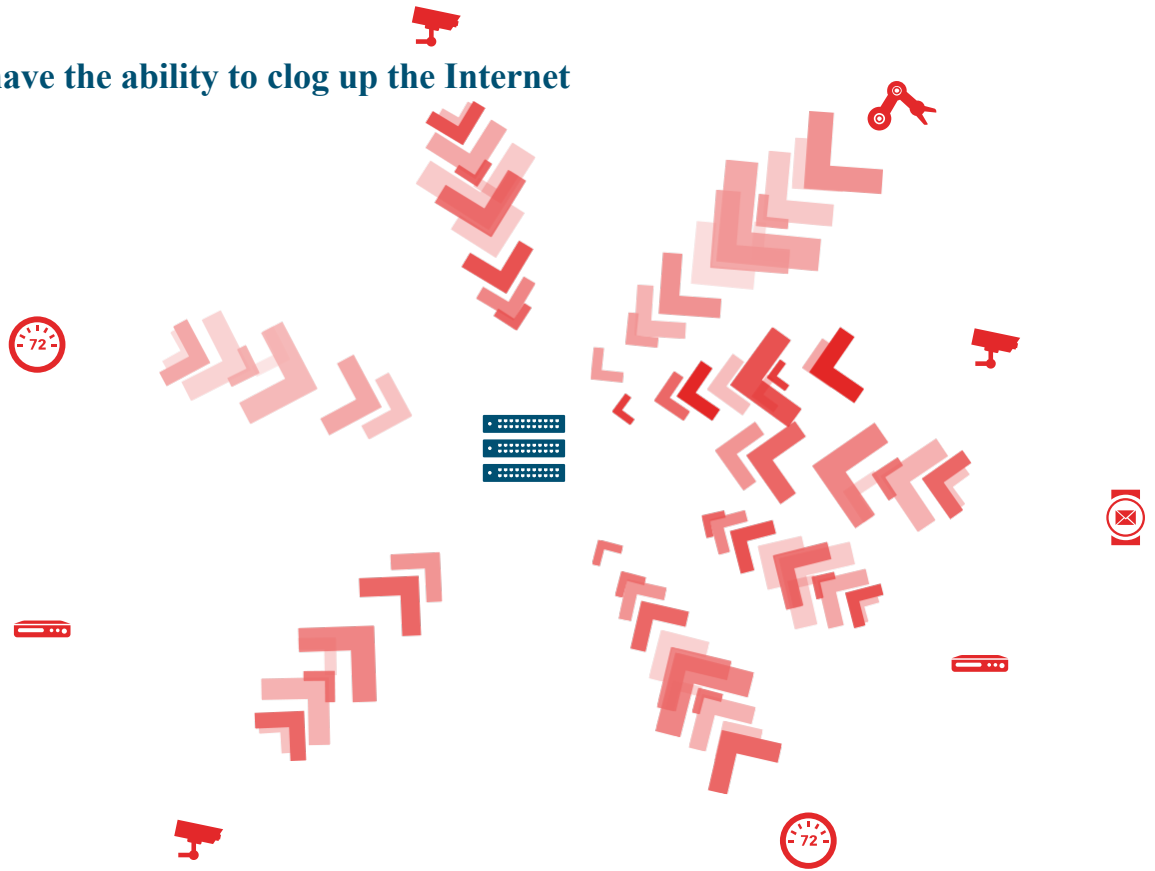
Ransom Denial of Service (RDoS)

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

DDoS

Botnets compete to control IoT and have the ability to clog up the Internet

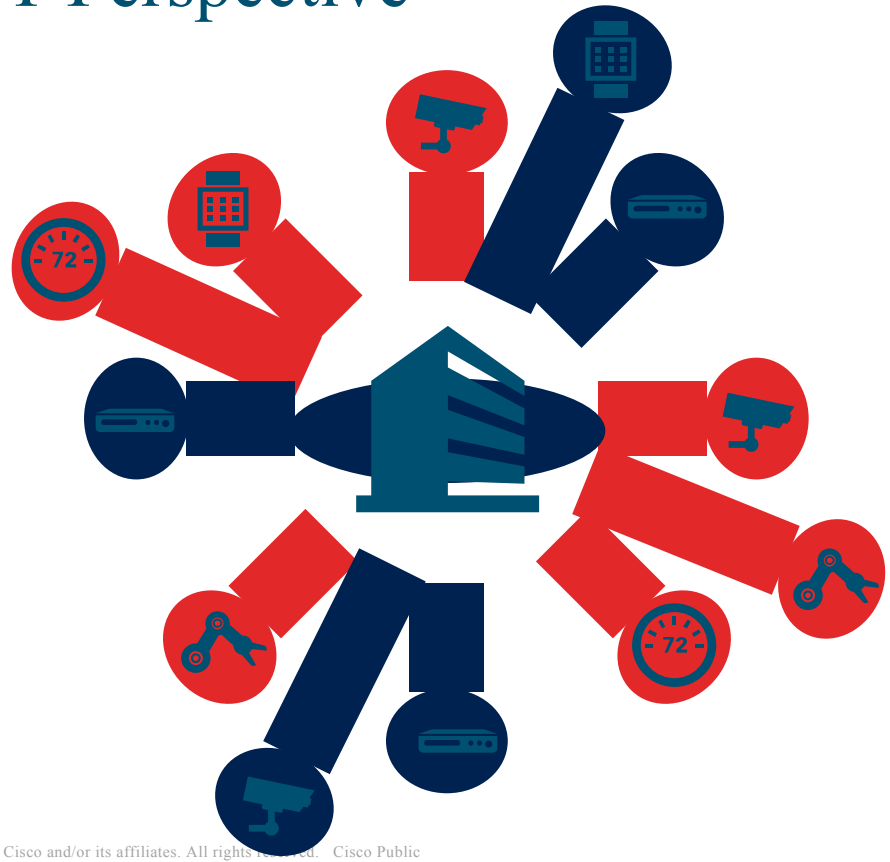
- IoT DDoS attacks propelled us into the 1TBps DDoS era
- Set up can be completed within an hour
- Distribution is rapid. Perpetrators can have a botnet of 100,000+ infected devices in 24 hours.
- The malware has a low detection rate. It is very difficult to retrieve samples because the malicious code lives in the device's memory and is wiped out once the device is restarted.



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source: Radware

IoT Perspective



- Moving from IT to OT
- Visibility issue
- Low hanging fruit for attackers
- Lagging behind desktop security
- Running insecure apps

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

Breach Readiness

- Maintain business continuity
- Protect your reputation and employee morale
- Avoid fines, legal fees, and remediation costs

I need a plan for when a data breach occurs.

I need to know what is in my network.

The Incident Response Plan

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Breach Response

Policies

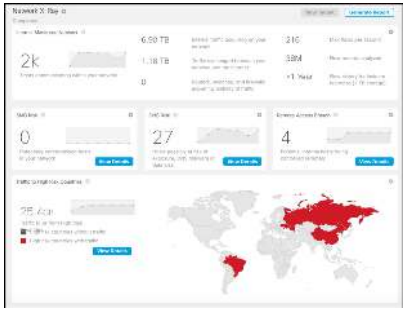
Processes

Technology

- Detect and Contain
- Remediate

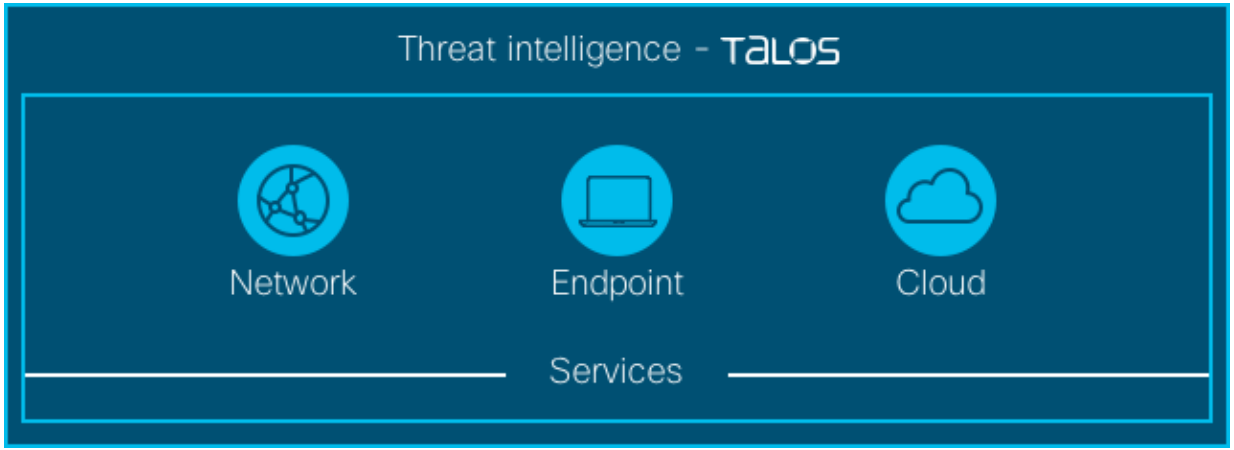
First line of defence

Protect your endpoints



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Can we help?



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

Talos

THREAT INTELLIGENCE

1.5 MILLION
Daily Malware Samples

600 BILLION
Daily Email Messages

16 BILLION
Daily Web Requests

Internet-Wide Scanning

Product Telemetry

Honeypots

Vulnerability Discovery (Internal)

Open Source Communities

INTELLIGENCE SHARING

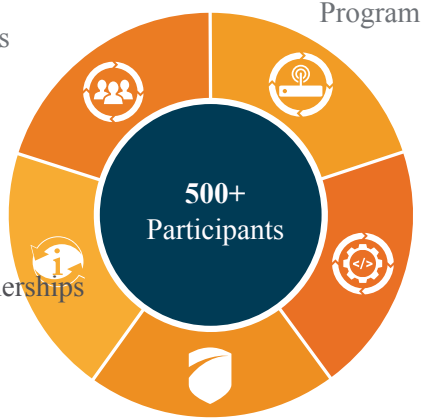
Customer Data Sharing Programs

Service Provider Coordination Program

Industry Sharing Partnerships (ISACs)

Open Source Intelligence Sharing

3rd Party Programs (MAPP)



300+
Full Time Threat Intel Researchers

MILLIONS
Of Telemetry Agents

4
Global Data Centers

100+
Threat Intelligence Partners

1100+
Threat Traps

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion

- The escalating impact of security breaches
- The defender is getting overwhelmed
- Influencing executive leadership
- Simple, open, and automated

Breach Readiness & Response

cisco


CISCO