Cyber Security for an IoT World

Presenter: David De Lima, BE, BSc, CENG (IET), CCIE 7958, CISSP, CISA

dadelima@cisco.com

Title: Consulting Systems Engineer – Security, Cisco Systems

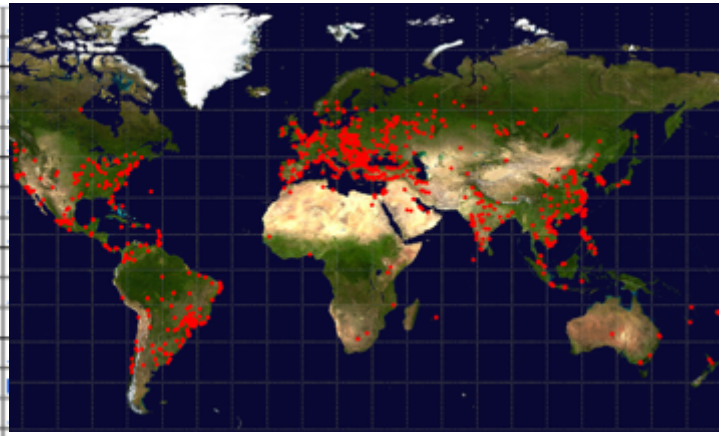
Date: May 2017

IoT Growth - 1.5 Million Devices Per hour!!

Mirai Botnet (IoT) Oct 2016

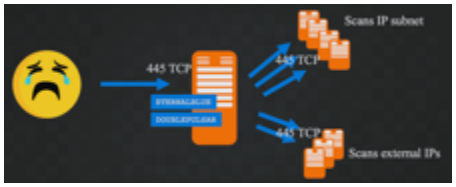
- Compromised IoT Devices
  - Baby monitors, webcams
  - Home routers
  - DVRs, printers
- Massive DDoS Botnet (600Gb-1Tb)
  - **DynDNS** attack (Liberia, Deutsche Telek
  - DDoS as a service, DDoS for ransom
  - Source code released!!
- **Challenges (why does it exist??)**
  - **Default Passwords, open ports, unma**
  - **Vulnerabilities (slow to patch)**
  - **Low focus on security (time to market**
  - **Low resources (CPU/RAM/Storage/etc**

ACTi IP Camera
ANKO Products DVR
Axis IP Camera, et. al
Dahua Camera
Dahua DVR
Dahua DVR
Dahua IP Camera
Dahua IP Camera
Dahua IP Camera
Dreambox TV receiver
EV ZLX Two-way Speaker?
Guangzhou Juan Optical
H.264 - Chinese DVR
HiSilicon IP Camera
HiSilicon IP Camera
HiSilicon IP Camera
HiSilicon IP Camera
IPX-DDK Network Camera
IQinVision Cameras, et al
Mobotix Network Camera
Packet8 VOIP Phone, et al
Panasonic Printer
RealTek Routers
Samsung IP Camera
Shenzhen Anran Security Camera
SMC Routers
Toshiba Network Camera
Ubiquiti AirOS Router
VideoIQ
Vivotek IP Camera
Xerox printers, et al
ZTE Router

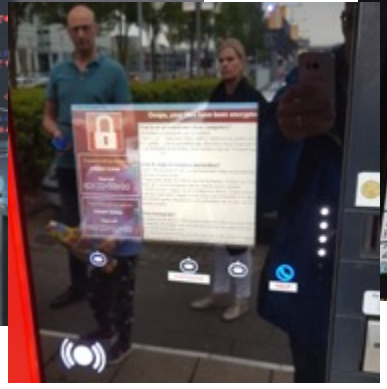


- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Swedish Civil Contingencies Agency[27]
- Swedish Government[27]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[28]
- Vox Media[29]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[30]
- WWE Network[31]
- Xbox Live[32]
- Yammer[23]
- Yelp[13]
- Zillow[13]

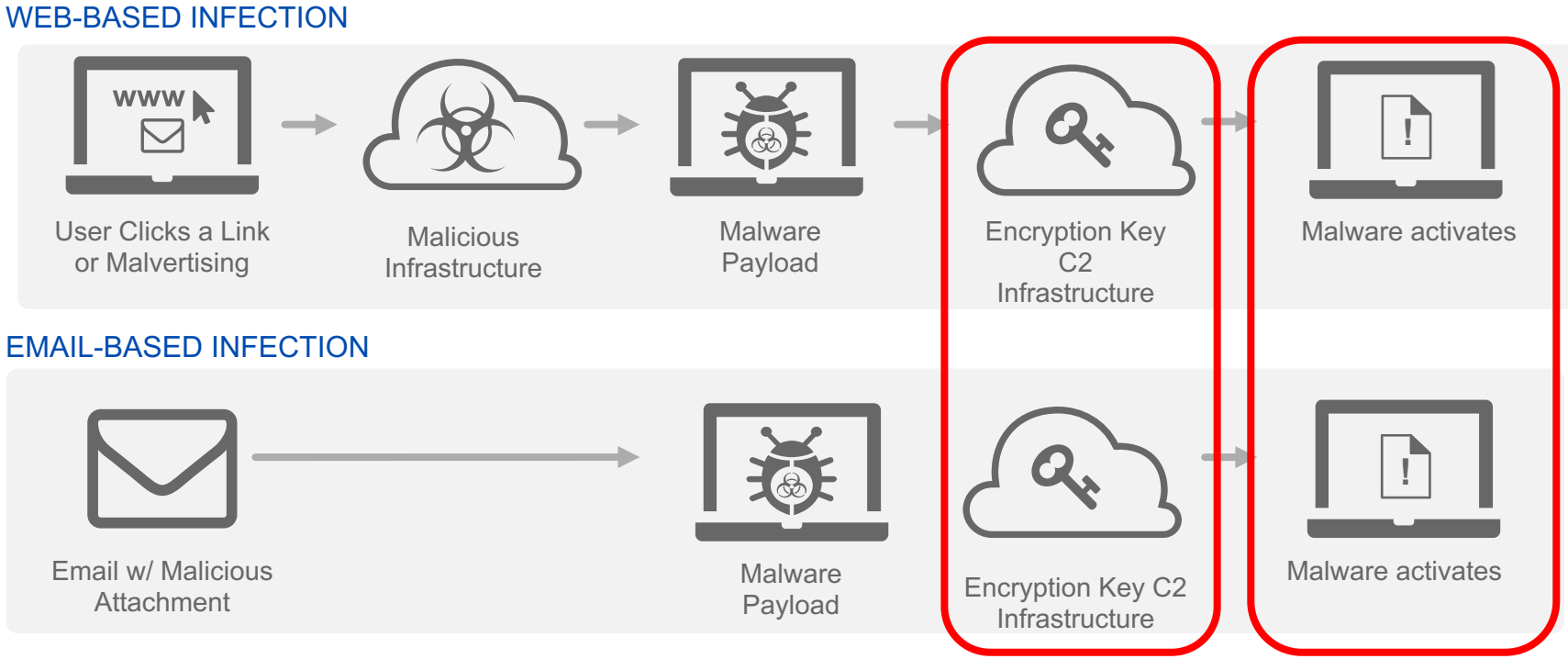
WannaCry (Worm – OT/IoT Impact)



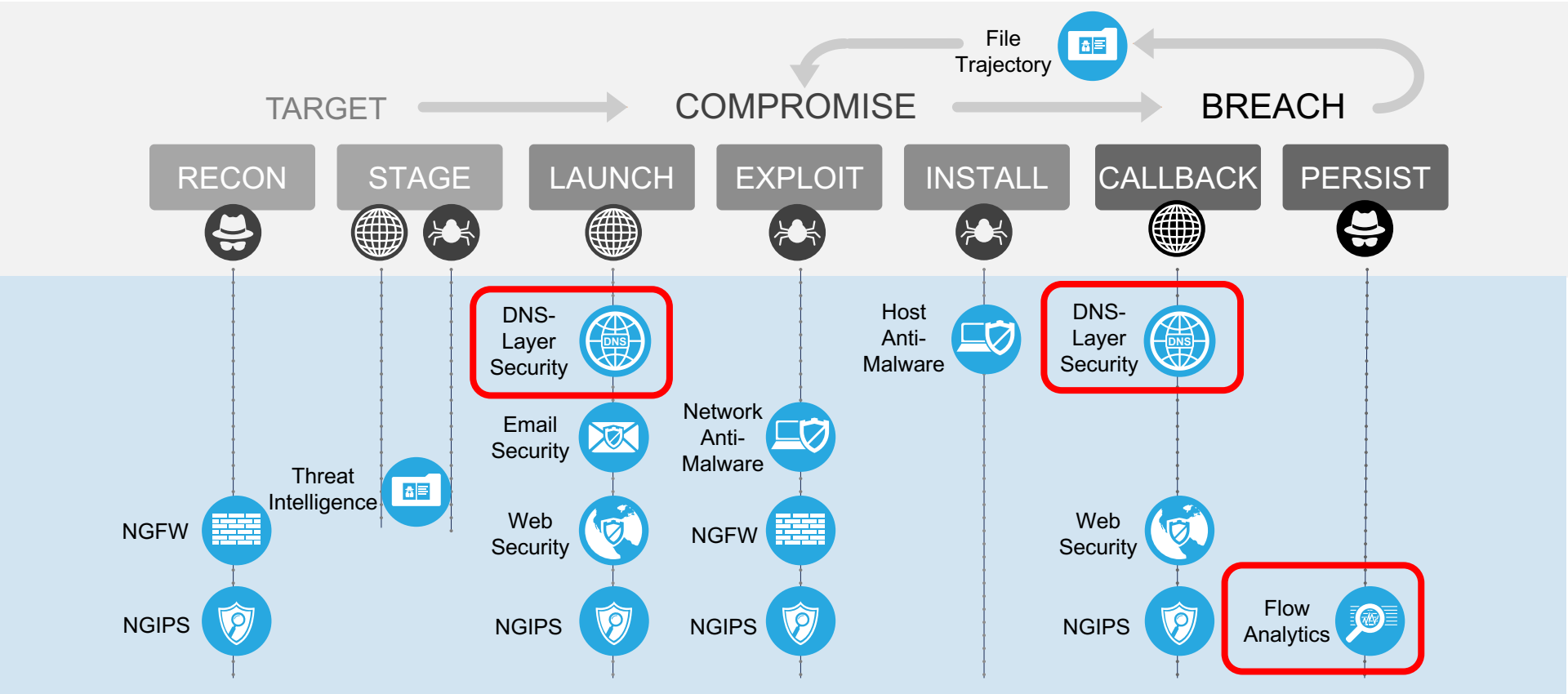
- Began on May 12 - spreads as a worm – 230,000 infections across 150 countries
- OT Impact - Britain NHS (computers, MRI scanners, blood-storage refrigerators and theatre equipment), Telefonica, Deutsche Bahn, Nissan (UK), Renault, ATMs, Parking Meters
- Exploits windows (MS17-010) using tools leaked by Shadow Brokers – 1 month head start!!
  - Not very sophisticated!! – Payment via 4 BTC wallets + AntiVM kill-switch + Direct Infection
  - Next one much worse (already new variants) - Mirai + Wannacry!! (DDOS kill-switch!!)



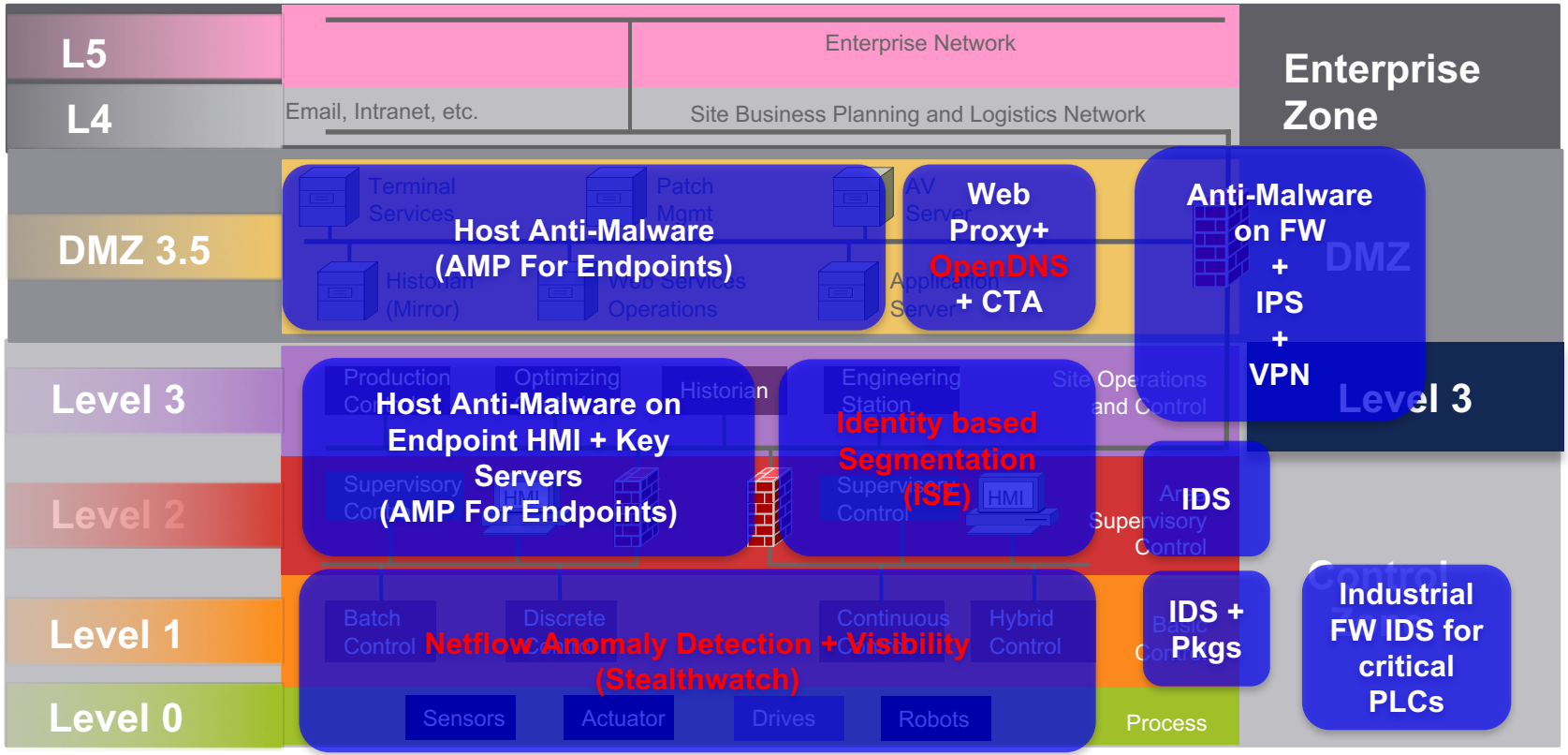
How Malware Works–Most Variants Require All 5 Steps



End-to-End “Kill Chain” Defense Infrastructure



OT Security Layers



DNS = Domain Name System

www.google.com = 172.217.26.68 (IP Address)

"OpenDNS FREE"

https://signup.opendns.com/homefree/

CNC = C2 = Command and Control

Monetise Malware (RAT, Banking Trojan, Ransomware, etc)

66.96.146.129 (IP Address)

www.evil.com = 66.96.146.129

Fast Flux IP

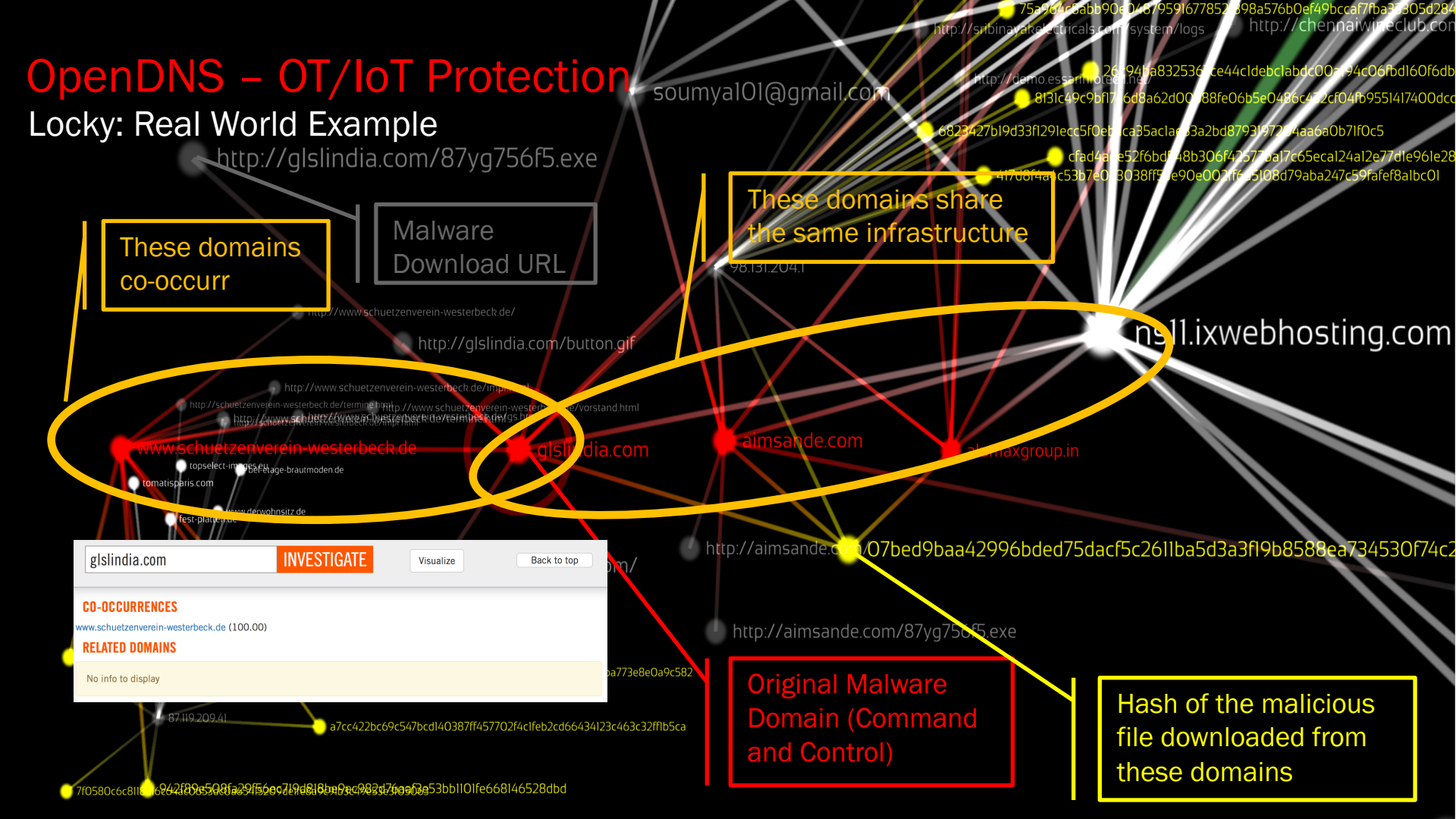
= 66.96.146.129 (2 hours later)

yfrscsddkkdl.com (Initial)
qgmcgoqeasgommee.org (2 hours later)
iyyxtyxdeypk.com (2 hours later)
diiqngijkpop.ru (2 hours later)

DGA – Domain Generation Algorithm

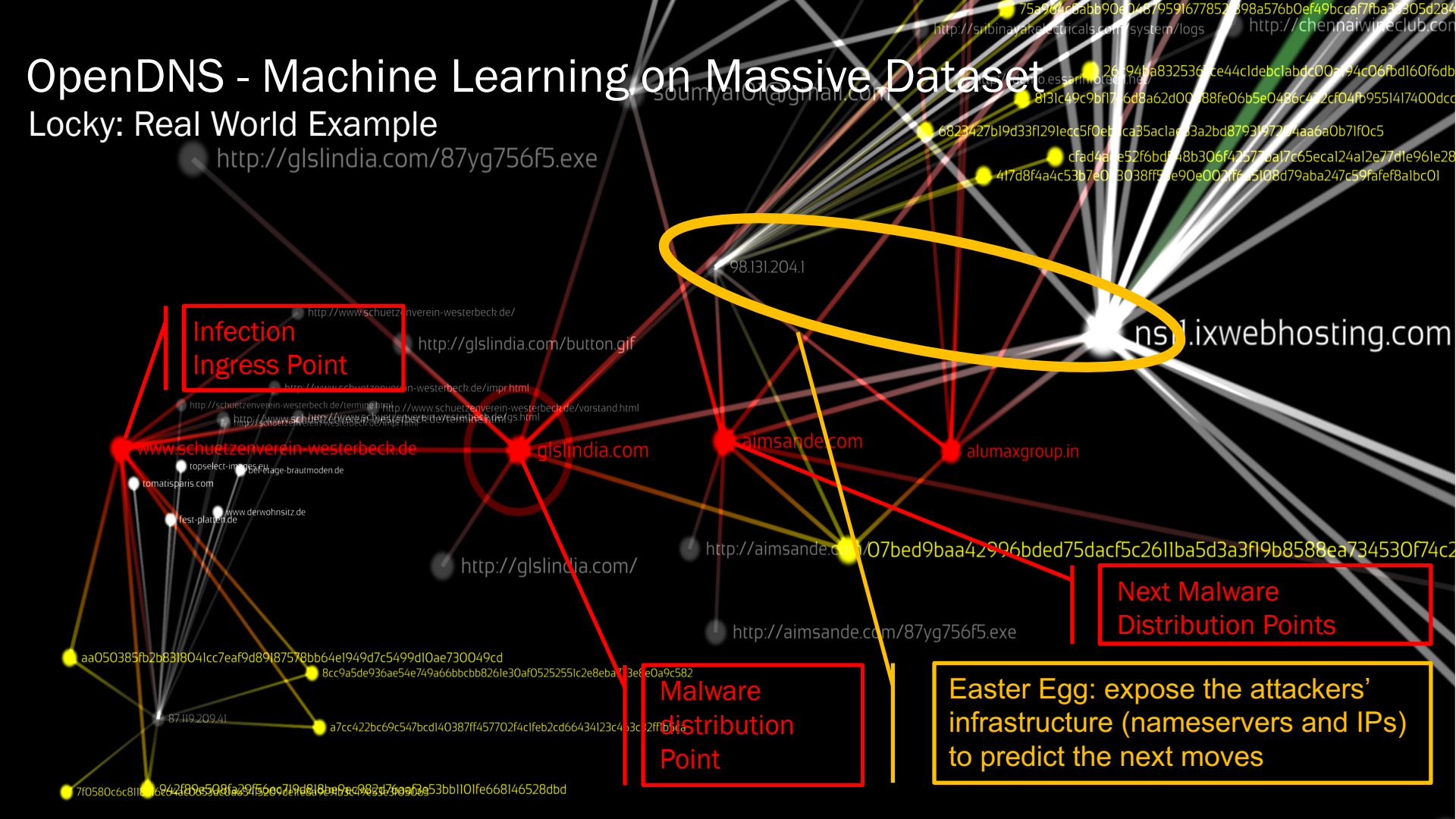
OpenDNS – OT/IoT Protection

Locky: Real World Example

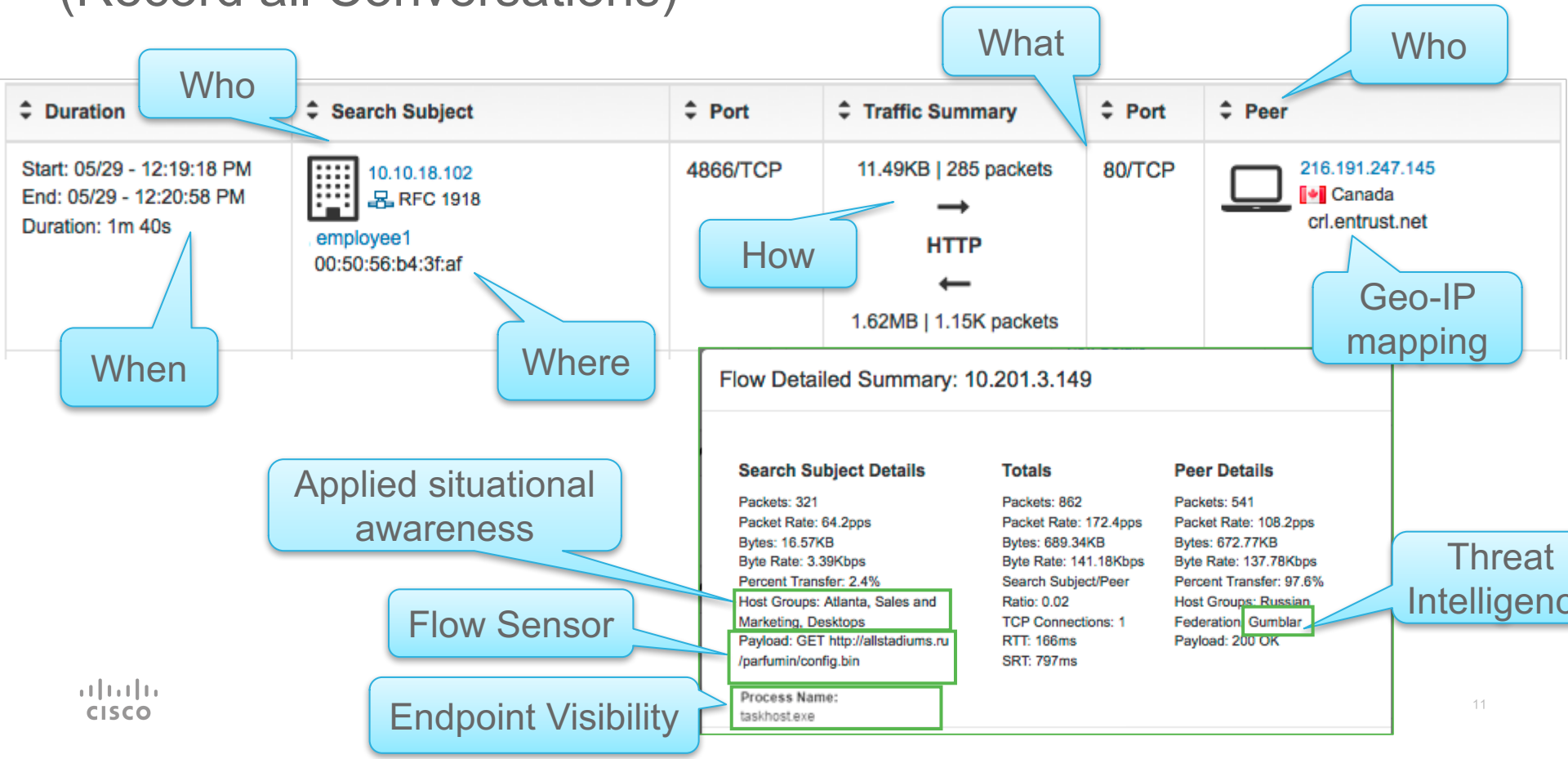


OpenDNS - Machine Learning on Massive Dataset

Locky: Real World Example

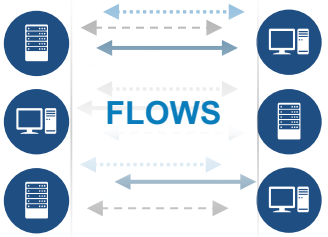


Stealthwatch – OT/IoT Protection
(Record all Conversations)



Stealthwatch - Behavioral and Anomaly Detection Model

COLLECT AND ANALYZE FLOWS



SECURITY EVENTS (94 +)

Addr_Scan/tcp
Addr_Scan/udp
Bad_Flag_ACK**
Beaconing Host
Bot Command Control Server
Bot Infected Host - Attempted
Bot Infected Host - Successful
Flow_Denied
.
.
ICMP Flood
.
.
Max Flows Initiated
Max Flows Served
.
Suspect Long Flow
Suspect UDP Activity
SYN Flood

ALARM CATEGORY

- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

RESPONSE

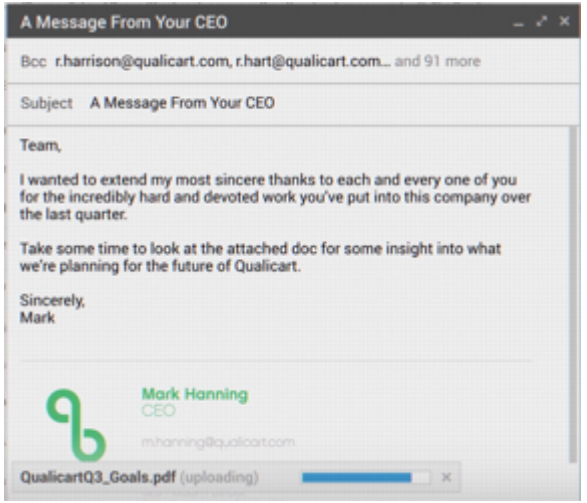
- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

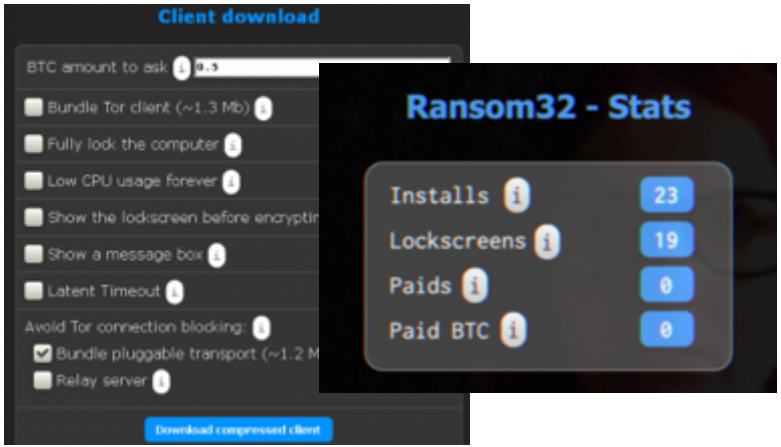
Anatomy of a Cyber Attack

https://www.youtube.com/watch?v=4gR562GW7TI

What did you notice??

- Attackers are not necessarily nerds in hoodies sitting in the dark
  - Commercial enterprises – well resourced – run as 9-5 companies
  - Free wifi, public space
- (Spear) Phishing attack (email attack)
  - Social engineering
  - Qaullcart.com vs Qualicart.com
  - Email signature
- Ransomware (smokescreen)
  - Ransomware as a service (Ransom32)
  - Pyramid affiliate schemes
  - Very popular – crypto currencies + anonymous web
- Real target - gamed stock, customer information





How can you help protect your organisation?

1. You are a target – be vigilant at all times (Social Engineering)
2. Don’t open up unknown attachments!! (Emails!! + Personal)
3. Understand what qualifies as sensitive data within your organisation (assets)
4. Backup data (work and personal)
5. Understand how to identify and avoid threats (skeptical mindset + phone)
6. Understand your organisation’s acceptable use policies
7. Understand your organisation’s security policies
8. If you’re ever in doubt – ask for help!


CISCO