NEW TOOLS OF THREAT HUNTING

Benny Ketelslegers

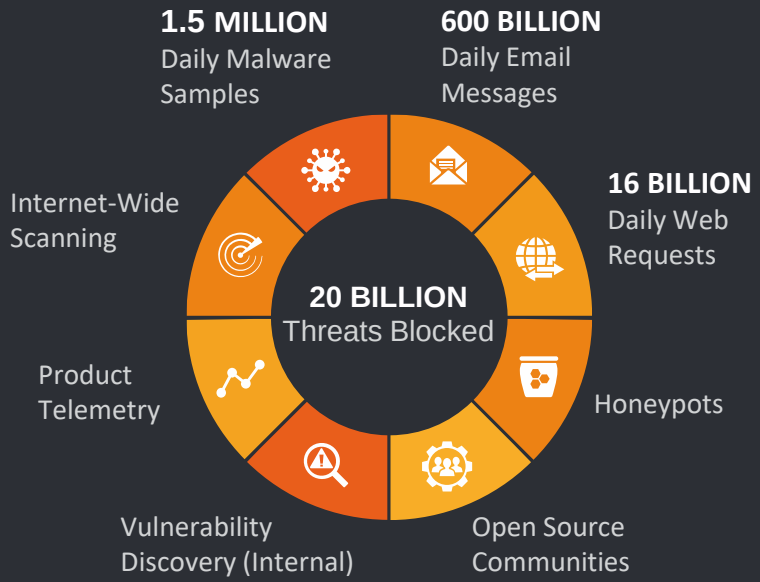
Industry-leading threat intelligence. The largest threat detection network in the world.

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）

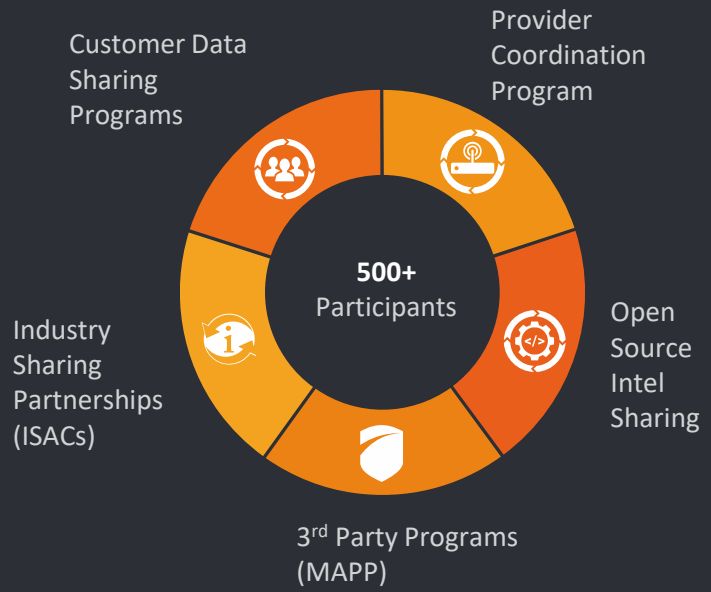
The importance of Threat Intelligence and how Cisco Talos uses intelligence to protect customers

Talos Intel Background

THREAT INTEL



INTEL SHARING



250+
Full Time Threat Intel Researchers

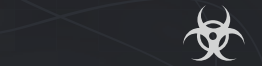
MILLIONS
Of Telemetry Agents

4
Global Data Centers

100+
Threat Intelligence Partners

1100+
Threat Traps





Intelligence Lifecycle

and the threat environment



Threat Intelligence

“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard ”

- Gartner

TALOS

Threat Intelligence

What are the bad guys up to that we don't already know about?

- Understand the threat environment
- Follow trends
- Detect new things first!

TALOS

Threat Intelligence

MIROX -
Carding,lobby,vente-

@MiroxGhostSquadHackers

Like Follow Share ...

Like Comment Share

MIROX -Carding,lobby,vente-
18 July ·

Pour faire un achat il vous suffit de m'envoyés un message
email juste ici ---> r00t.nosecure01@gmail.com !
Shop ==> https://m.facebook.com/profile.php... !

See Translation

Like Comment Share

5

I will test your website for DDOS

$5

I will solve your DDOS attack

$5

I will stress test and Massive DDoS Attack your Website

$5

I will professional stress test your web site with DDos

$5

TALOS

Ask Yourself

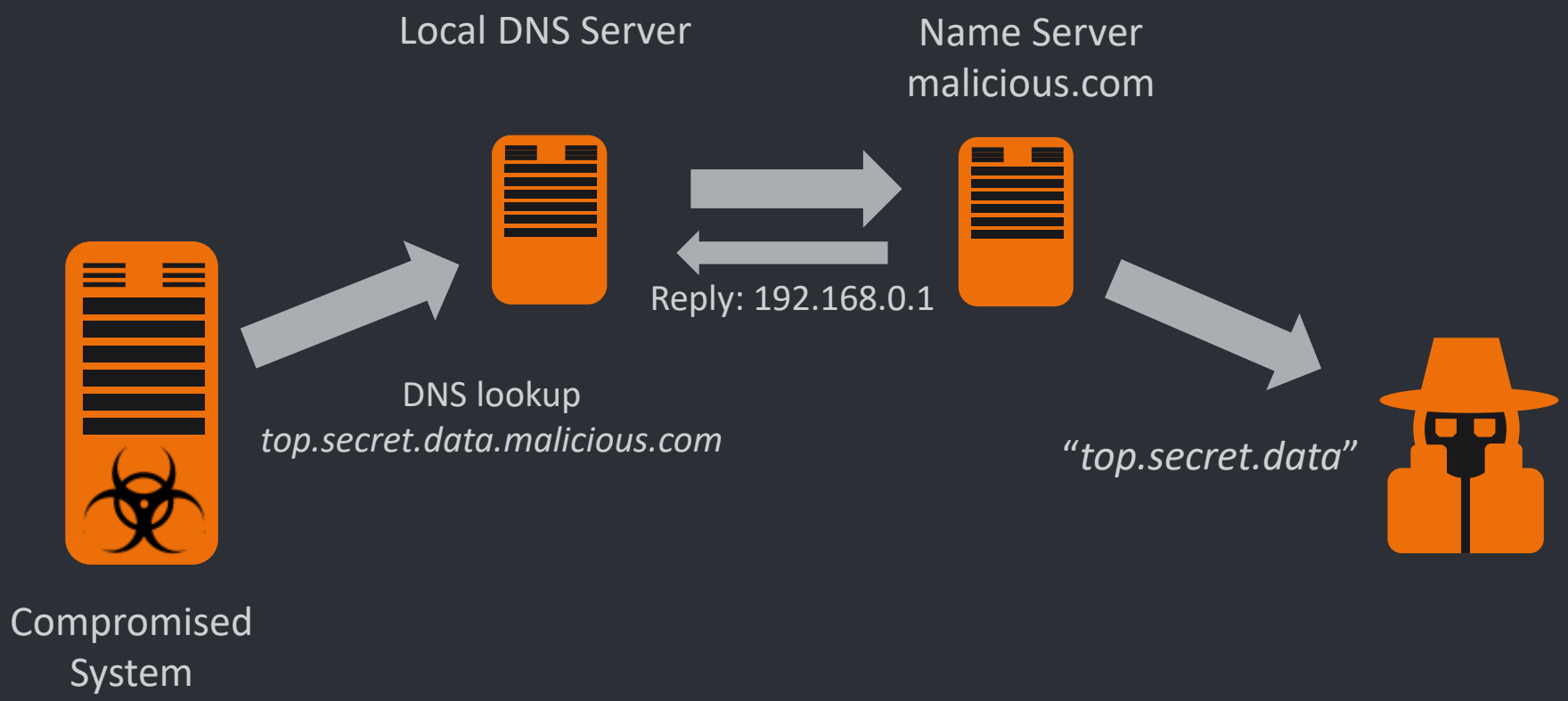
What might be happening?
What evidence might exist?

How would I find out?

Threat Intelligence in Action

Exfiltration by DNS

EXFILTRATING DATA BY DNS



TALOS

EXFILTRATING DATA BY DNS

DNS lookup problems:

- Punctuation forbidden
- Case insensitive

Base32 Encoding

“top secret data” ➔ ORXXAIDTMVRXEZLUEBSGC5DB

“Top Secret !!!!” ➔ KRXXAICTMVRXEZLUEAQSCIJB

DNS Requests

www.domain1.com

mail.domain2.com

server.*xyz*.domain3.com

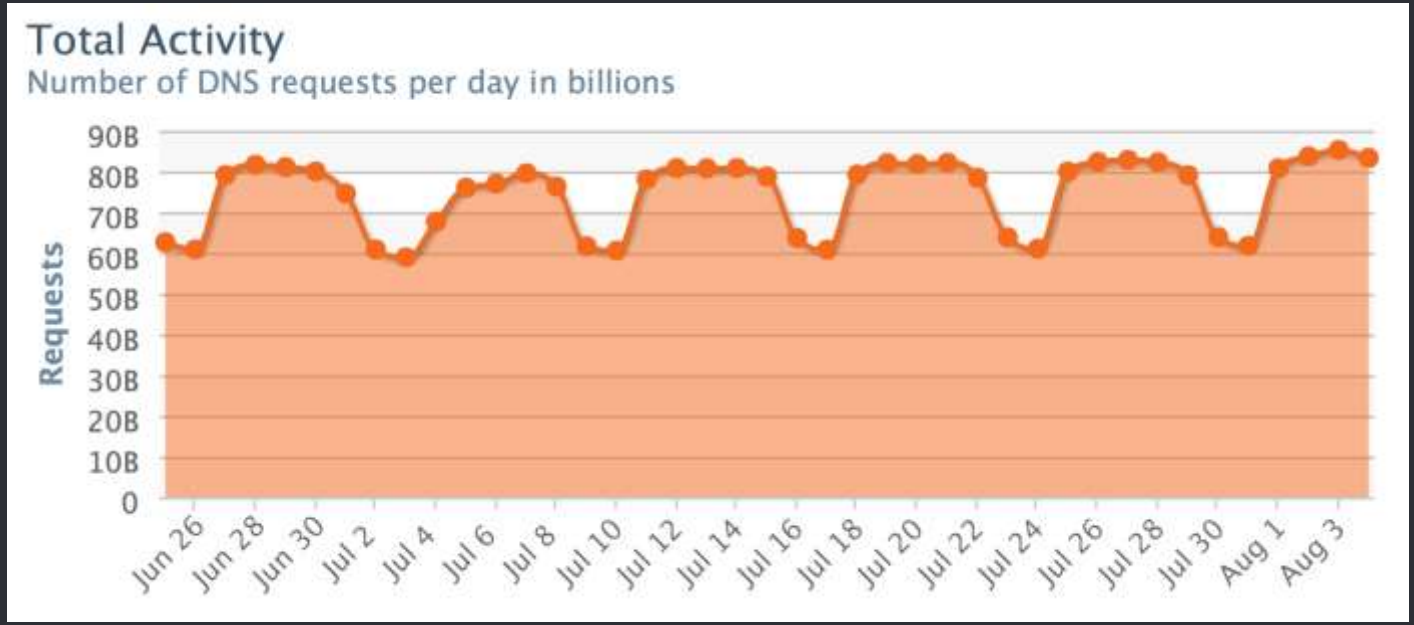
ORXXAIDTMVRXEZLUEBSGC5DB.malicious.com

TALOS

LETS GO HUNTING!

Lets look for ‘long’ domain names.

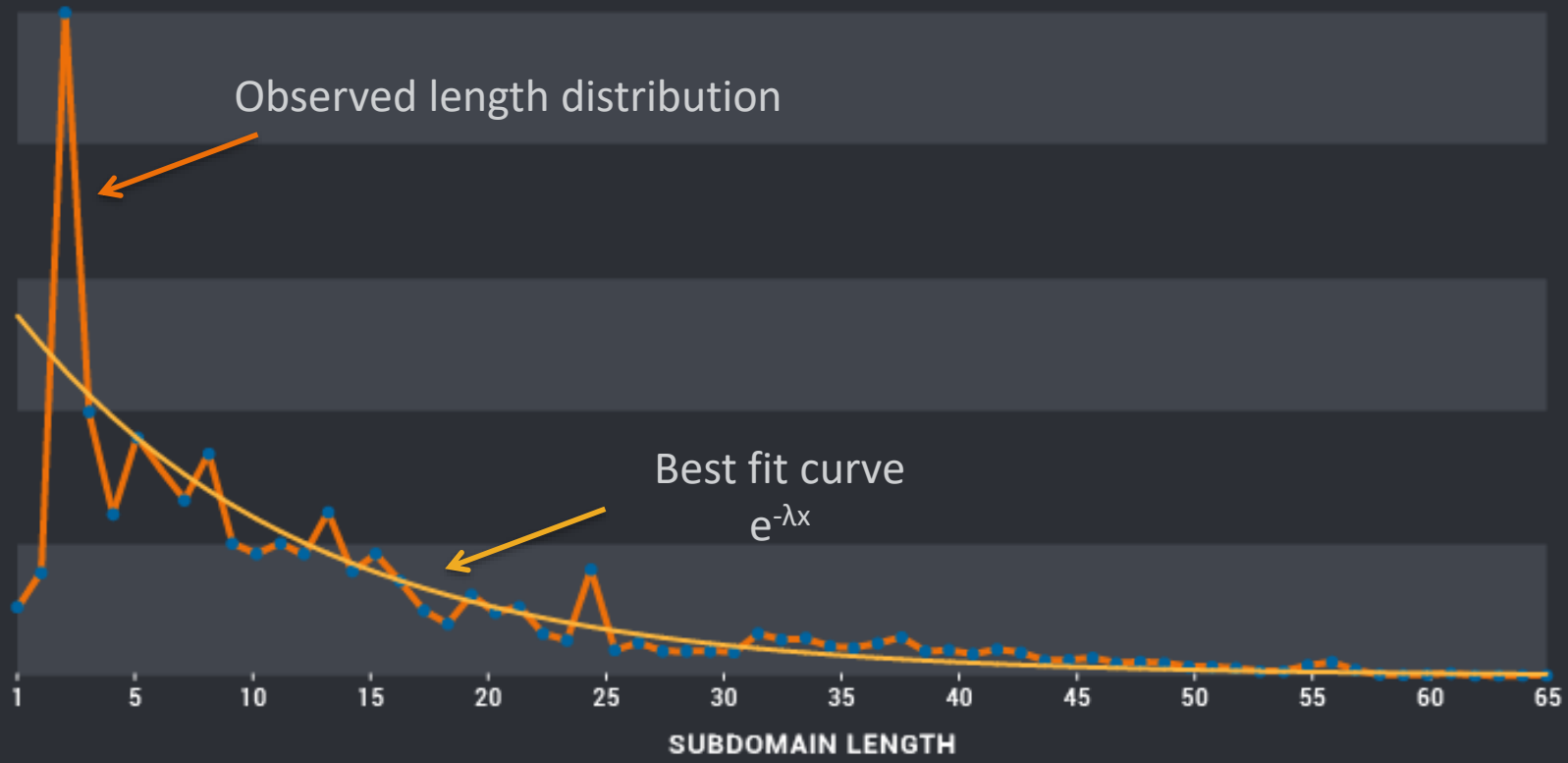
Oh great there are 100 million!



OpenDNS DNS Lookup Data

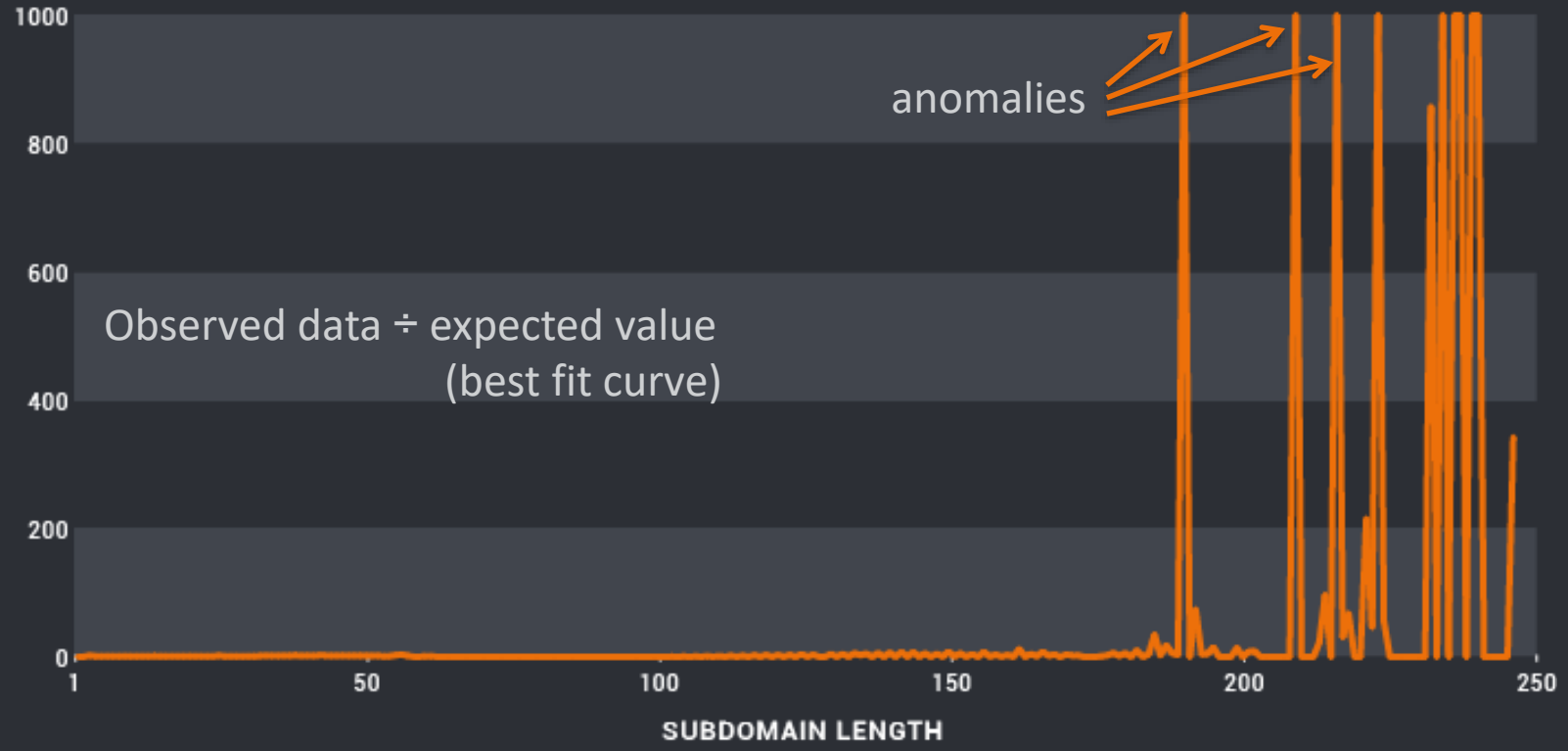
TALOS

MODEL DATA



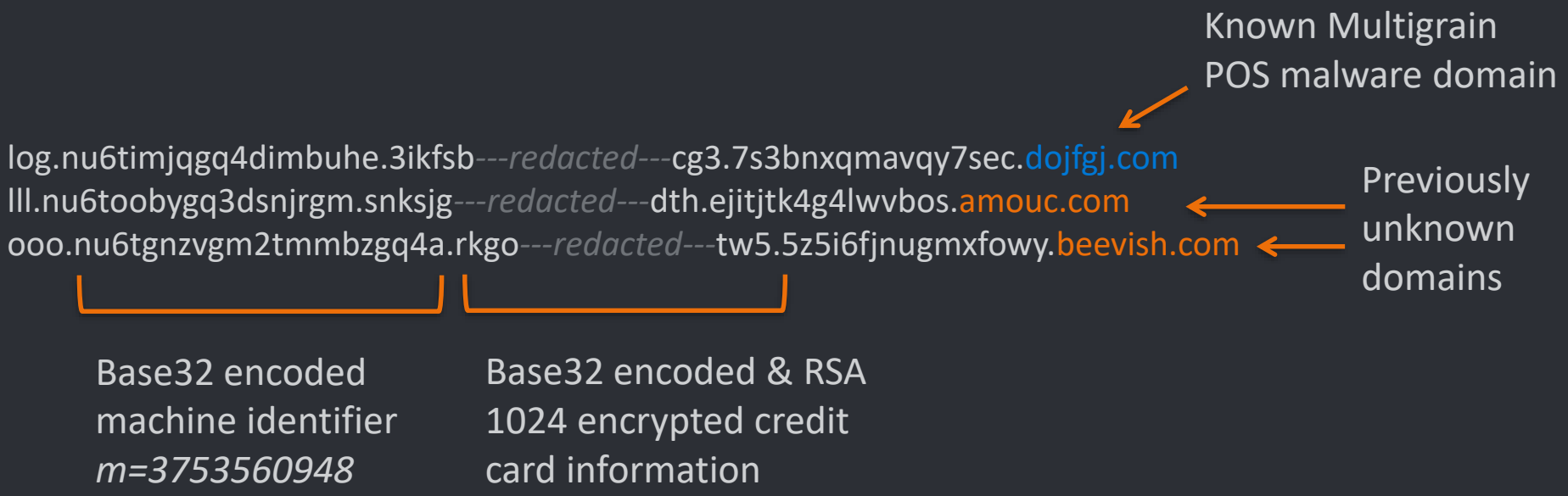
TALOS

IDENTIFY ANOMALIES



TALOS

ACTIVE EXFILTRATION




VPNFilter

Background

- For several months Talos researchers have been collaborating with public- and private-sector threat intelligence partners and law enforcement to research a threat named “VPNFilter”

- VPNFilter is a campaign that deploys a multi-stage malware system to SOHO router and network devices around the world.

- More than 500,000 infections

- VPNFilter stage 2 has a kill command that potentially would disable infected devices.

Targeted Devices

QNAP

LINKSYS®

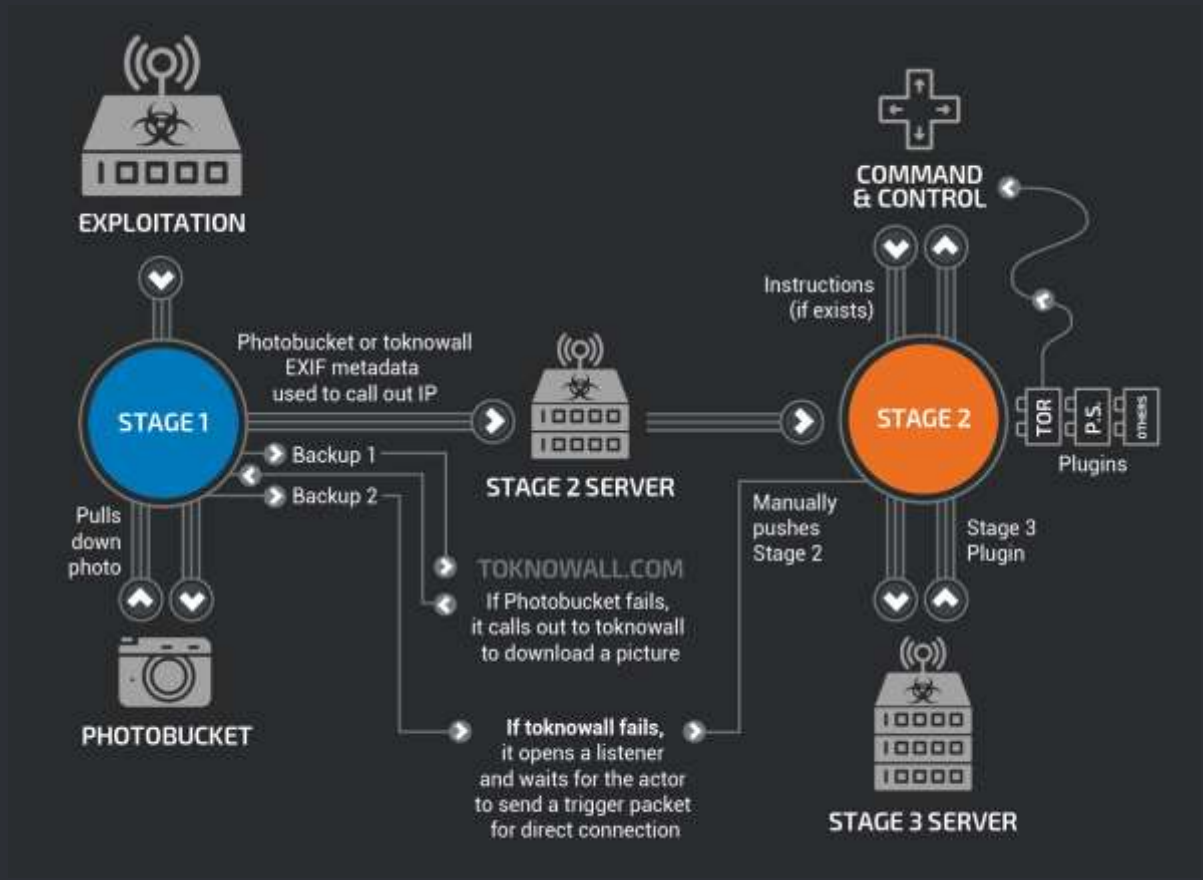
HUAWEI

MikroTik

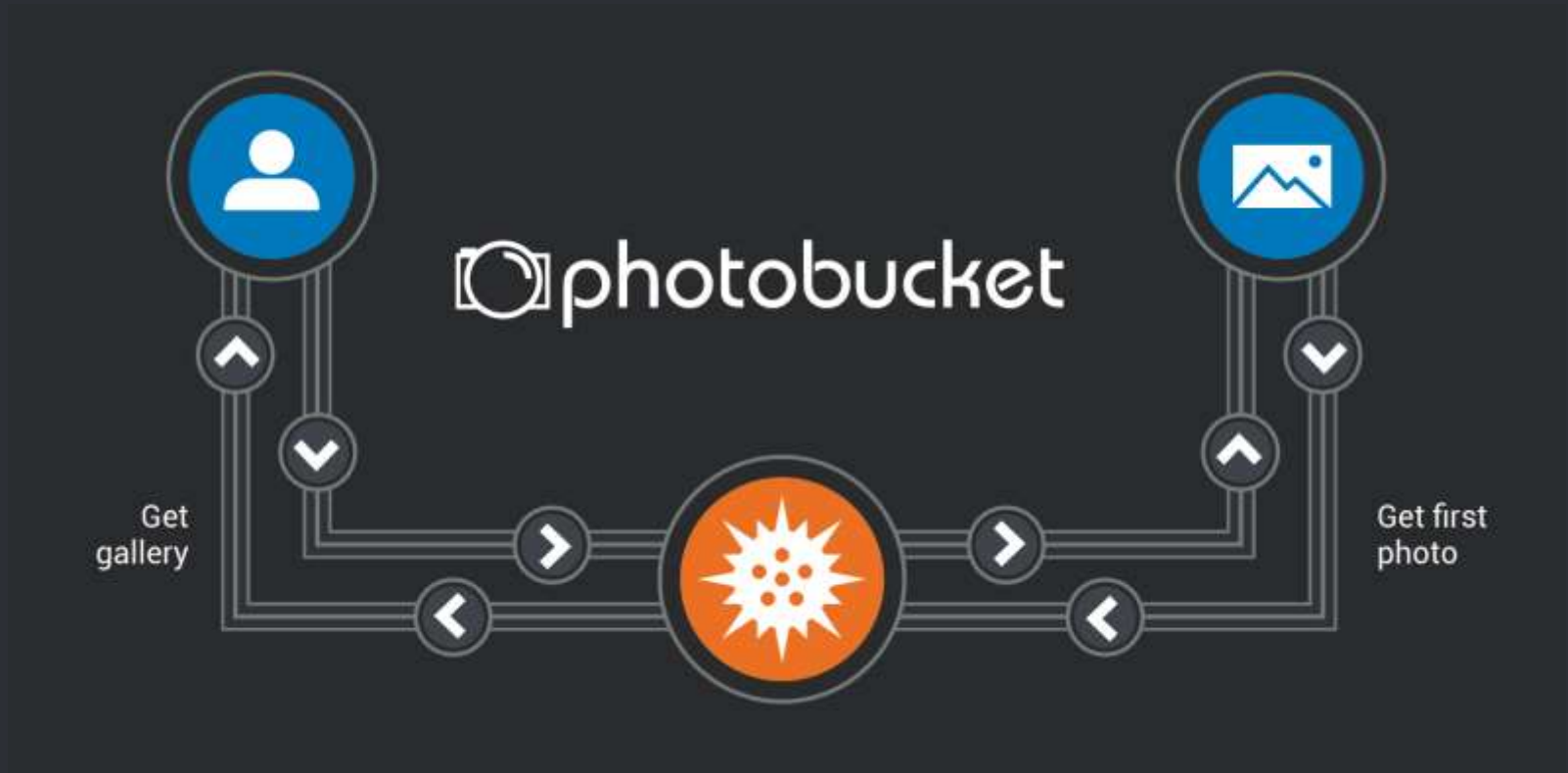
UBIQUITI NETWORKS

NETGEAR

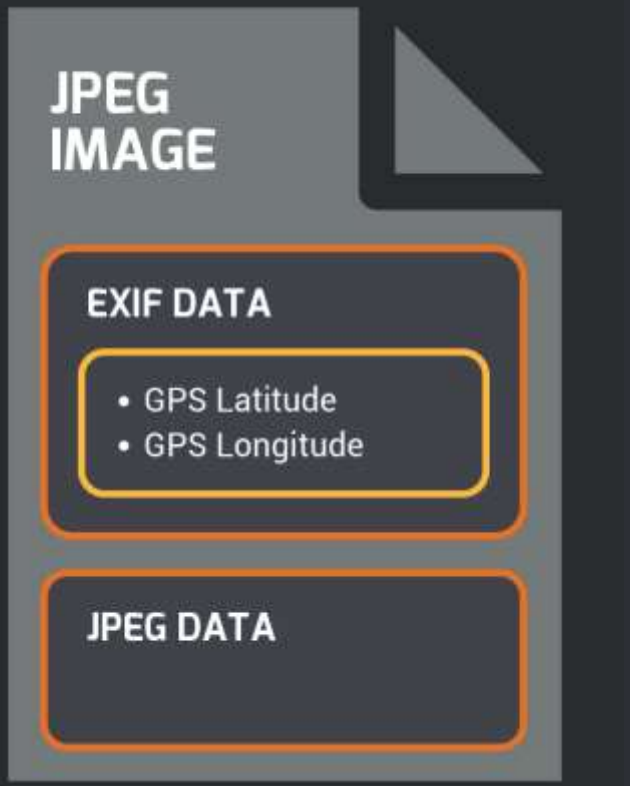
Infection Process



Stage 1

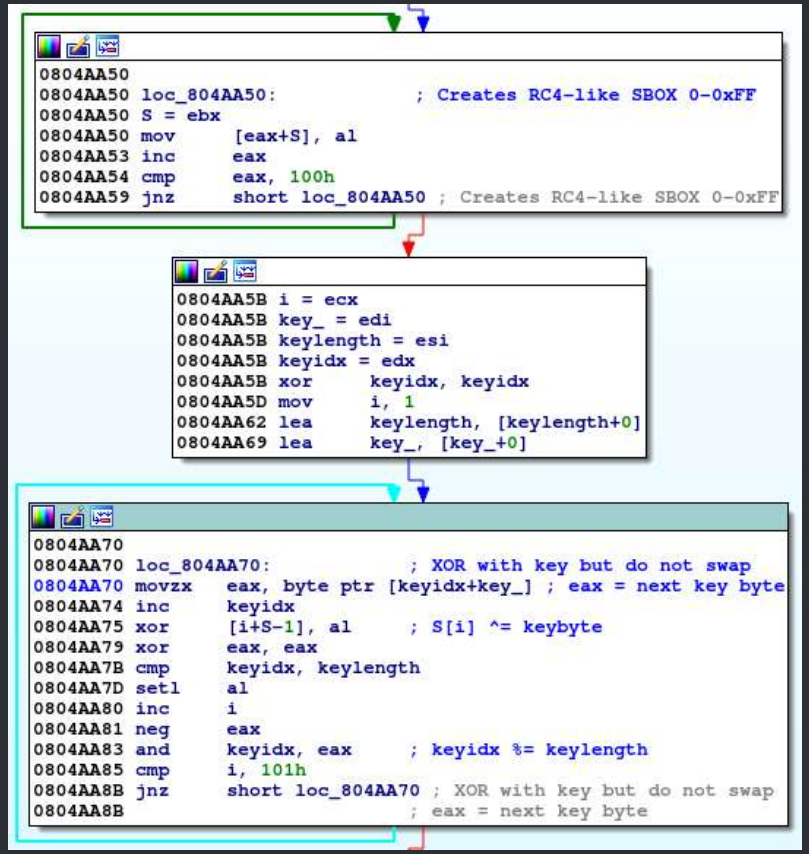


Stage 1



- EXIF data containing GPS coordinates used to identify Stage 2 server.
- If this process fails, the malware reaches out to toknowall[.]com to obtain IP address.
- If the backup fails, the malware opens a listener for the attacker to directly connect to the device.

Stage 1



- Leverages crontab for persistence.
- C2 leverages Tor or SSL-encrypted communications.
- Same RC4 implementation that was used by BlackEnergy.

Blackenergy

- First discovered 2007 with DDoS capability
- Version 3 actively used in 2014-15
  - known for having SCADA-related plugins
  - Heavily targeted Ukraine
- Blackenergy targets:
  - ICS, energy, government and media in Ukraine
  - ICS/SCADA companies worldwide
  - Energy companies worldwide

Stage 2

- Not persistent across device reboots.
- Reaches out to C2 infrastructure to obtain commands to execute on infected devices.
- Provides all the functionality an attacker would need to deploy additional malware stages to infected devices.

Stage 2 - Functionality

- The x86 version of Stage 2 can perform the following functions:
  - kill: Overwrites first 5,000 bytes of /dev/mtdblock0 with zeros and reboots the device.
  - Exec: Executes shell command or plugin.
  - Tor: Sets the tor configuration flag (0 or 1).
  - Copy: Copies a file from the client to the server.
  - Seturl: Sets the URL of the current configuration panel.
  - Proxy: Sets the current proxy URL.
  - Port: Sets the current proxy port.
  - Delay: Sets the delay between main loop executions.
  - Reboot: Reboots the device.
  - Download: Downloads a URL to a file.

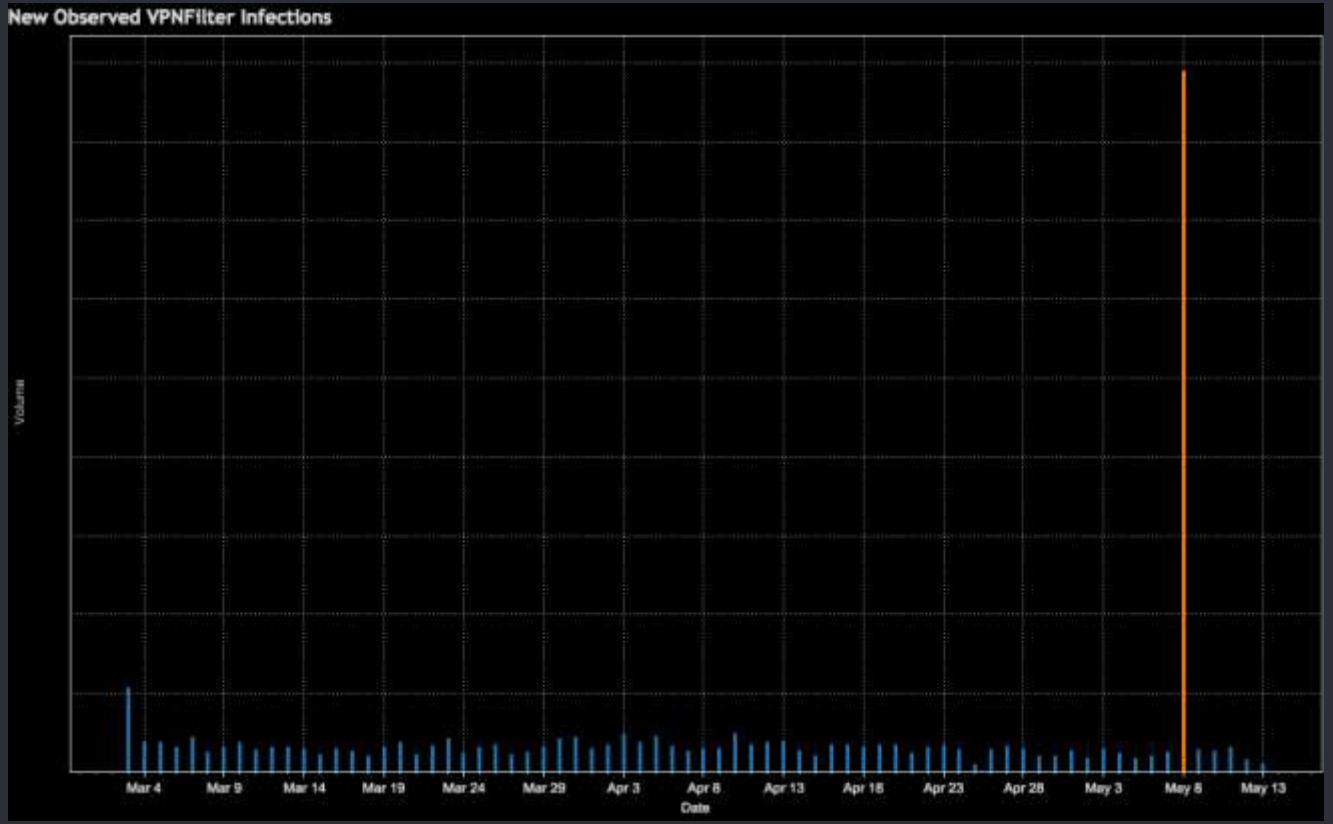
- The MIPS version of Stage 2 has these additional operations:
  - Stop: Terminates the malware process
  - Relay: A misspelled version of the “delay” command described above.

Stage 3

- Not persistent across device reboots

- Includes modules to:
  - Enable C2 communications using the Tor network.
  - Capture and save traffic transferred through infected devices.
  - The malware specifically tracks Modbus packets transmitted over IP.

Infections over Time



Findings

- Have identified data exfiltration from affected systems.
- Have identified additional scanning from devices on TCP/23, TCP/80, TCP/2000, TCP/8080.
- Code overlap with BlackEnergy V2 and V3.
- Published Snort signatures targeting known vulnerabilities in devices targeted by VPNFilter

Conclusions

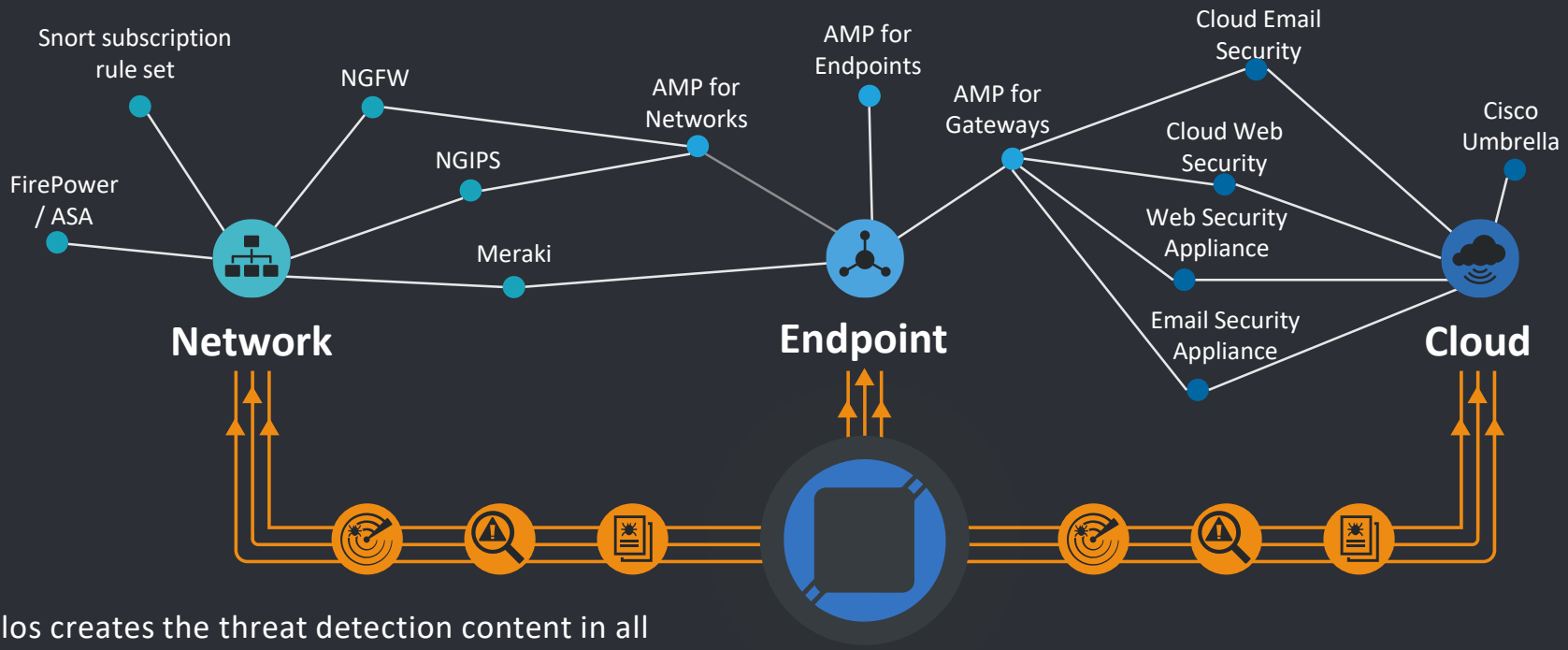
- VPNFilter is an expansive, robust, highly capable, and dangerous threat that targets devices that are challenging to defend.

- Device wiping functionality could be leveraged to impact internet connectivity for hundreds of thousands of victims.

- IOT and embedded devices are increasingly attractive to attackers hoping to collect information and stay under the radar.

Threat Intelligence

The Backbone of Cisco Security



Talos creates the threat detection content in all Cisco Security products, providing customers with comprehensive solutions from cloud to core.

TALOS

Enabling the Good Guys

Spreading security news, updates, and other information to the public

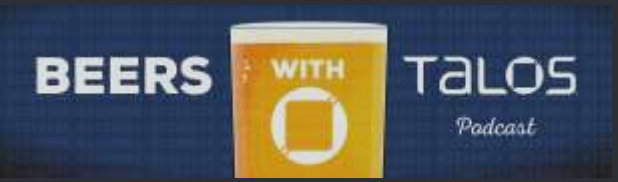
White papers, articles, & other information
talosintelligence.com

ThreatSource Newsletter
cs.co/TalosUpdate

Talos Blog
EN:blog.talosintelligence.com
CN:https://www.cisco.com/c/zh_cn/products/security/talos.html

Social Media Posts
Facebook: TalosGroupatCisco
Twitter: @talossecurity

Instructional Videos
cs.co/talostube



Download on iTunes

GET IT ON Google Play

TALOS

Open Source

Public Facing Tools

- Threat detection and prevention: Snort, ClamAV, Razorback, Daemonlogger & MBRFilter
- Threat Research: LockyDump, FIRST
- Vulnerability detection and mitigation: Moflow, FreeSentry

TALOS

Local Contacts

徐洪涛(Hongtao Xu)

思科大中华区安全业务技术总监

Email :hongtxu@cisco.com

扫描二维码，

获取更多**ISC2018**会议资料！

talosintelligence.com
blog.talosintel.com
@talossecurity