

Risikoen med "ting"

Nils Roald

Cisco Advanced Threat Group – Northern Europe

Intelligence

Best of breed
Portfolio



Integrated
Architecture

All hackers targeting your
infrastructure has one
common goal..

ENDPOINTS

Why endpoints is in focus again?



IoT exponential growth



Resource Hijacking



Growth in encrypted traffic



Requirement for visibility and traceability



To few resources

CRITICAL

The background of the image is a dark, industrial environment. It features various mechanical parts, including what appears to be a large metal flange or valve on the left side. The scene is illuminated with a strong blue light, creating a high-contrast, futuristic atmosphere. Several cables or hoses are visible, running across the frame. The overall composition suggests a complex, high-tech system.

IoT
ICS
Smart...

IoT attack surface

IoT Challenge

- Volume of Devices
- Operating Systems
- Designed to be (un)secure
- Protocols
- Immature usage





Tidligere bil i Visible Tesla



Ny bil i Teslas app

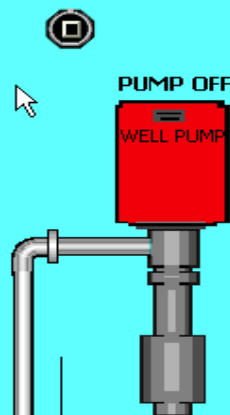
CITY OF SOUTH HOUSTON VIRGINIA WATER PLANT

LOGOUT DISMISS
PUMP INFORMATION

OPERATION MODE: PLANT IN PRIMARY

TO DISTRIBUTION SYSTEM

ETM PUMP RESET



TO GROUND STORAGE TANK

ENABLE	AUTO	HAND	HRS 0	MIN 32
ENABLE	DISABLE			

ENABLE	AUTO	HAND	HRS 0	MIN 50
ENABLE	DISABLE			

ENABLE	AUTO	HAND	HRS 0	MIN 47
ENABLE	DISABLE			

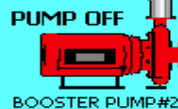
ENABLE	AUTO	HAND	HRS 16	MIN 24
ENABLE	DISABLE			



50.8 PRESSURE



BOOSTER PUMP#1



BOOSTER PUMP#2



BOOSTER PUMP#3



BOOSTER PUMP#4

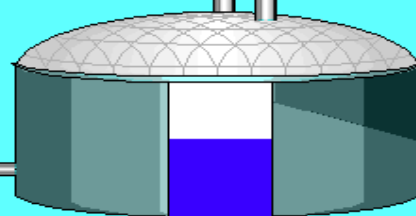
COMM GOOD

ENABLE	AUTO	HAND	WELL PUMP
ENABLE	DISABLE		
		HRS 0	MIN 0

ENABLE	AUTO	HAND	SWV VALVE
ENABLE	DISABLE		
		HRS 10	MIN 34

BOOSTER PUMP
ONPRESS OFFPRESS

LEAD	50.0	52.0
LAG#1	46.0	52.0
LAG#2	44.0	52.0
LAG#3	42.0	52.0
HIGH PSI ALARM	56.0	
LOW PSI ALARM	40.0	



17.2 GST LEVEL

TO GROUND STORAGE TANK

DAILY REPORT

FLOWMETER

621.4 g/m
TOT 842041000

VALVE OPEN

SW VALVE

FROM CITY OF HOUSTON

ONLEVEL OFFLEVEL

WELL PUMP	15.0	18.0
GST FILL VALVE	17.0	19.0

LO-LEVEL CUTOFF 8.0
HIGH LEVEL ALARM 22
LOW LEVEL ALARM 10

CITY MAP

ALARM

OPERATOR ID

sh

CASE ID

COOLDOWN

9 MINUTES

OVERRIDES

Master Timer

1 : 00

Afterburner

OFF

C. Burner #1

00 :30

Throat Air

01 :00

Hearth Air

00 :15

CASE INFO

Size:

Med (101-200) ▼

Container:

Cardboard ▼

Gender:

Male ▼

Case # of Day:

1 ▼

DEFAULTS

Infant

PRESET 2

PRESET 3

ELAPSED TIME 1:52

22 % OXYGEN

A/B

T/A

CB1

H/A

752 Deg

Datalog Enabled

ABORT

CYCLE START

EXIT



Dan Tentler 
@Viss

holy shit, I found a yacht.
do I win, @ydklijnsma? :D
(cc @shodanhq)

Following



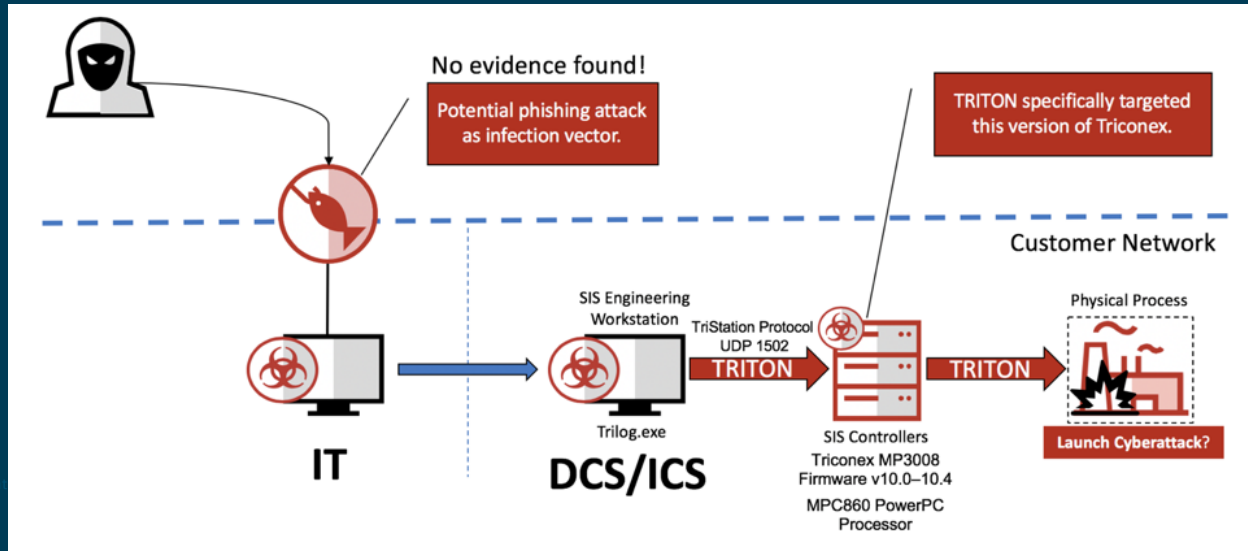
Some examples

CASINO



Triton

- Cause Operational Disruption to Critical Infrastructure
- Triconex Safety Instrumented System (SIS) controllers
- “The world’s most murderous malware”



Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!

■ . . .

```

      .
      @88>
      %8P
      .u
      .d88B :@8c
      ~.888: x888 x888.
      ~.888~'888X ?888f .@88u =~8888f8888r
      X888 888X '888> '888E 4888>'88~
      X888 888X '888> 888E 4888> '
      X888 888X '888> 888E 4888>
      X888 888X '888> 888E .d888L .+
      ~*88%~*88~'888! 888& ^~8888*~
      ~~~~~~
      R888~ ~Y~
      ~~~~~~

```

Username	Password
admin	admin
root	default
support	support
admin	password
root	root
root	12345
root	password
service	service
guest	guest
root	user
tech	tech
mother	fucker

- A text-based MUD by [Oscar P](#)

No account? Register at www.elrooted.com

Enter user> yop

yop

Enter pass> yop

Disconnected by server. |

Press any key to exit.



TRAVEL

United Will Soon Allow Some Cats and Dogs Back Into Its Cargo Holds. Here Are the New Rules.



LEADERSHIP

Arizona Teachers May Finally End Their Week-Long Statewide Strike



TECH

'Great for U.S./Russia Relationships:' Match Owner Takes Swipe at Facebook's Dating Business Ambitions



AUTOS

Tesla Hit With a \$2 Billion Lawsuit for Allegedly Stealing Nikola's Hydrogen Truck Design

TECH • PHIIPS

Light Bulbs Flash "SOS" in Scary Internet of Things Attack



Mike Kemp—Rubberball/Getty Images

By **JEFF JOHN ROBERTS** November 3, 2016

Hackers used a drone to target a set of Philips light bulbs in an office tower, infecting the bulbs with a virus that let the attackers turn the lights on and off, and flash an "SOS" message in Morse code.

You May Like

by **Outbrain** | ▶

Heidi Klum's New Penthouse Is "One Of The Last Of Its Kind"

by Mansion Global | Sponsored



If You Want to Job, Don't Say Any of These in an Interview

by Work+Money | Sponsored



The World's Richest Man Just Lost \$10.7 Billion as Trump Tweets About...



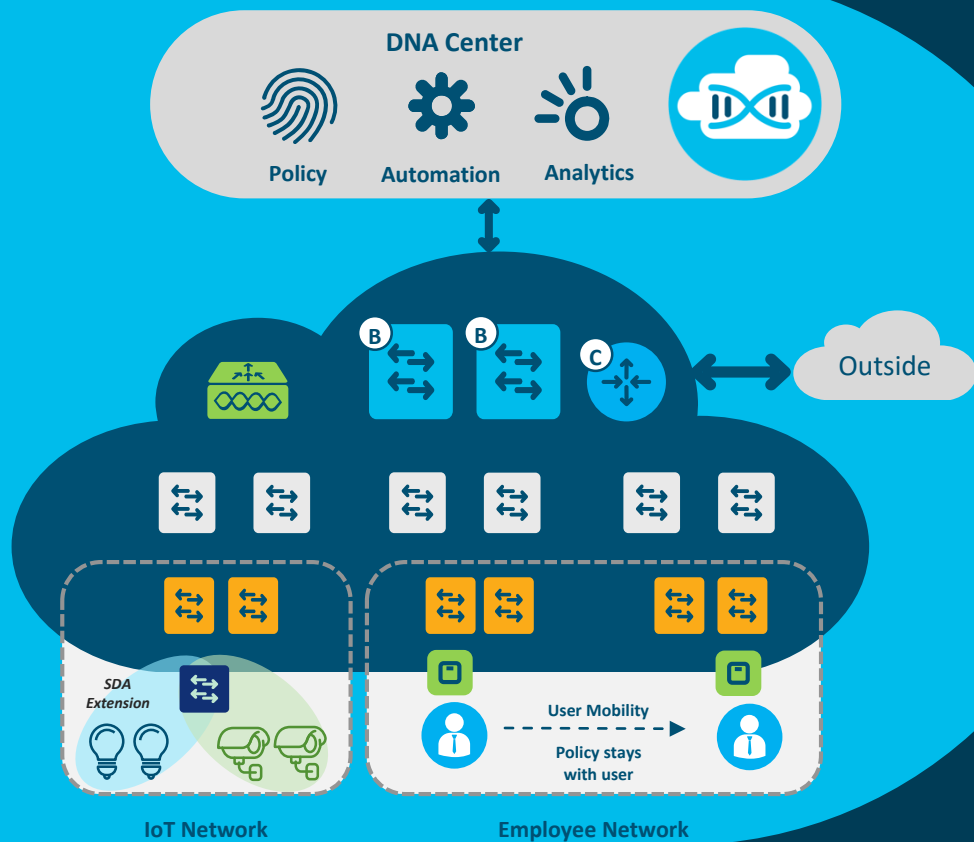
IoT attack goals

- Denial of Service
- Destroy
- Botnet
- Beachhead
- Manipulate data
- Spionage



Cisco IoT Security

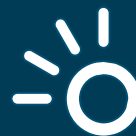
Segmentation



Identity-Based
Policy & Segmentation



Automated
Network Fabric



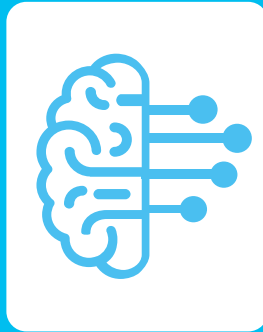
Insights
& Telemetry

New detection methods

Umbrella



Cognitive Analytics



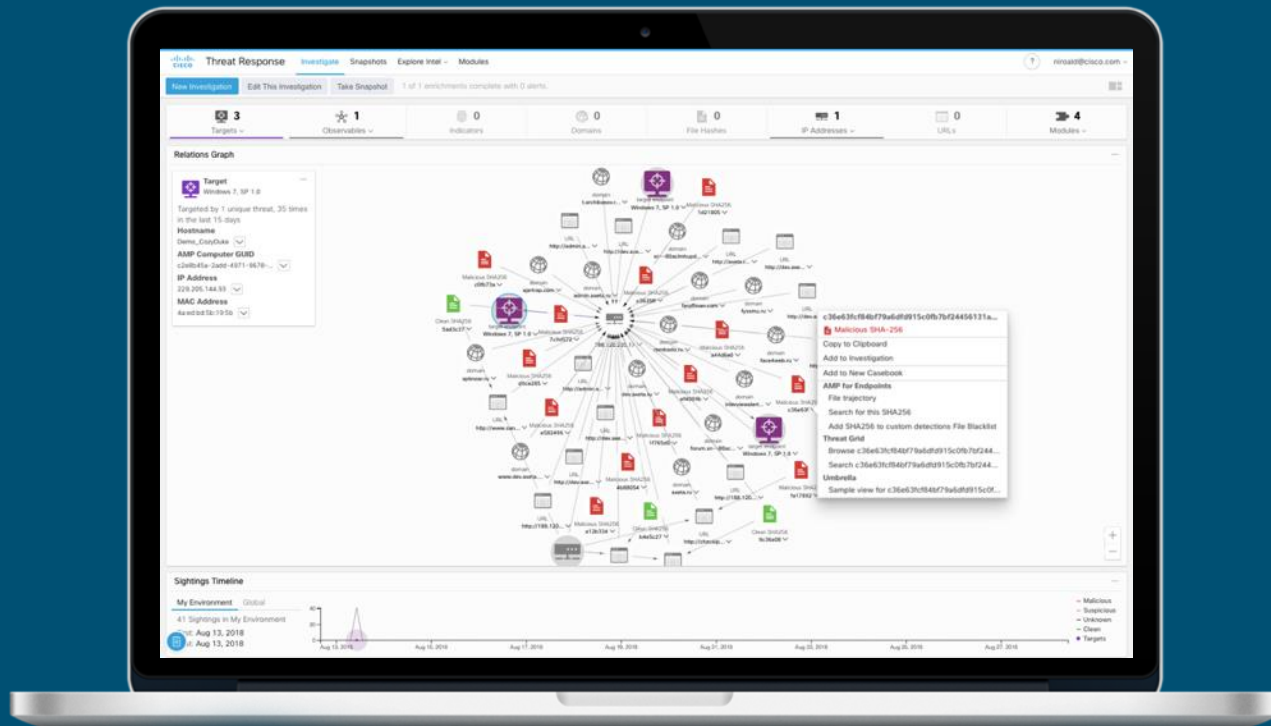
Stealthwatch



Agentless detection



Visibility



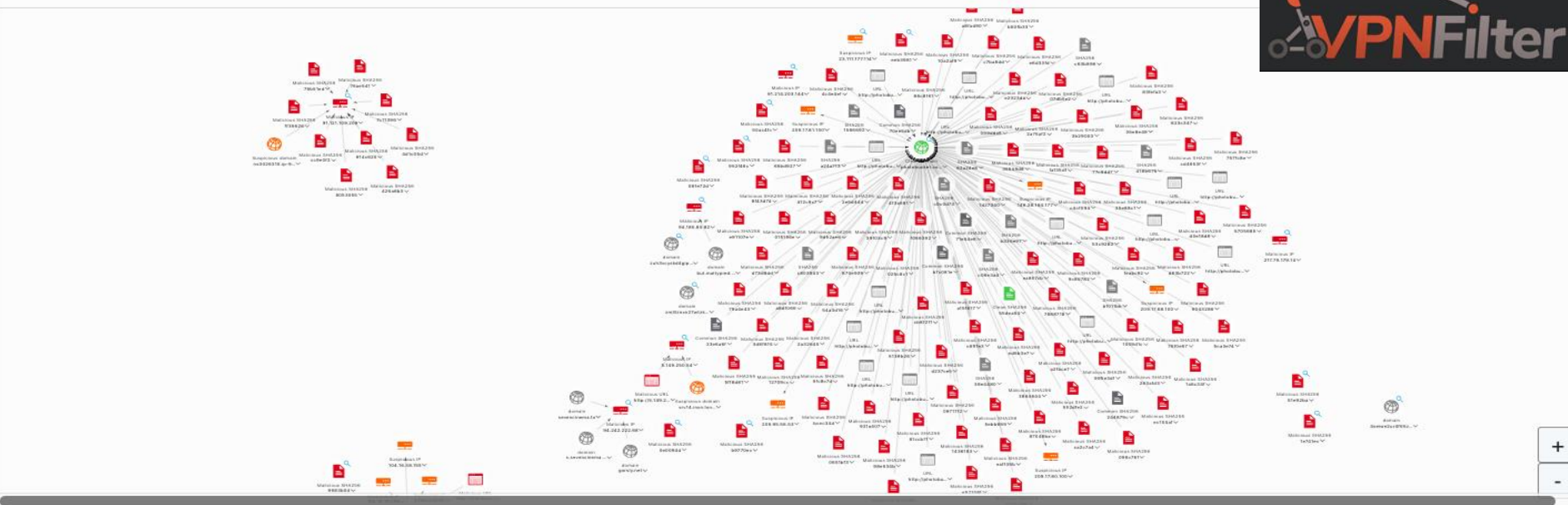
[New Investigation](#)
[Snapshots ...](#)

Stacked Layout

Investigation 48 of 48 enrichments complete

 0 Targets
  48 Observables
  0 Indicators
  7 Domains
  27 File Hashes
  14 IP Addresses
  0 URLs
  4 Modules

Relations Graph Showing 200 nodes



Sightings Timeline

[My Environment](#)
[Global](#)

24 Sightings


 st: Apr 1, 2013

st: Sep 24, 2018





