falcongate

info@falcongate.cz

fJ | falcongate

a Raspberry Pi powered gateway to stop Hackers, Malware and more

By
Leonardo Mokarzel Falcon
& Michal Meravy

ABOUT US

“The opinions and views expressed in this presentation are our own and not positions of our current employers”

Leonardo

- Husband and father of 3 girls
- Ex-bioinformatician
- Aficionado of all cyber stuff
- Currently infosec manager in a Fortune 500
- Developer and entrepreneur in his free time
- Public handles: Aesalon / A3sal0n

Michal

- Ex-Professional Athlete
- Information Technology Enthusiast
- Currently working as infosec specialist
- Dog lover, developer in his free time
- Public handles: easy4MEr

@FalconGate_GW

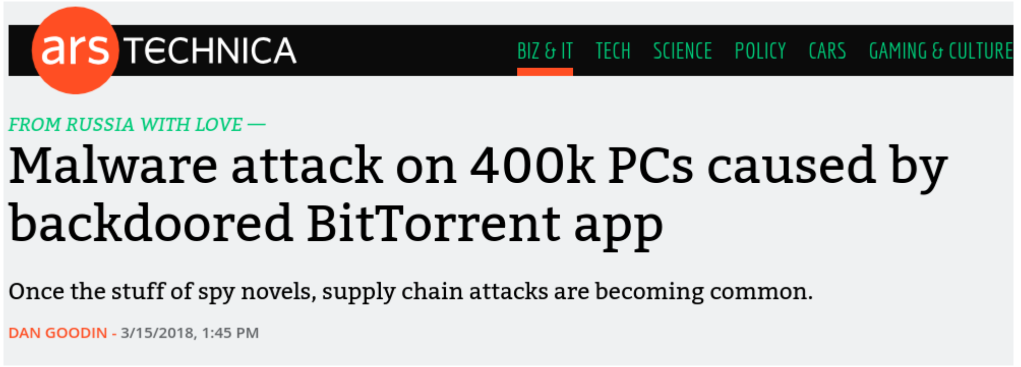
info@falcongate.cz

https://github.com/A3sal0n/FalconGate

https://www.facebook.com/falcongate.gw

THE PROBLEM

Small businesses, medium size companies and home users are defenseless against ransomware, IoT attacks and hackers

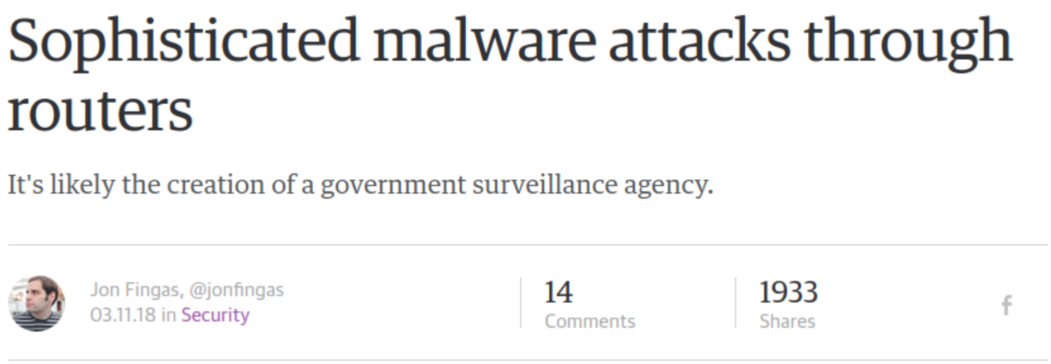


FROM RUSSIA WITH LOVE —

Malware attack on 400k PCs caused by backdoored BitTorrent app

Once the stuff of spy novels, supply chain attacks are becoming common.

DAN GOODIN - 3/15/2018, 1:45 PM



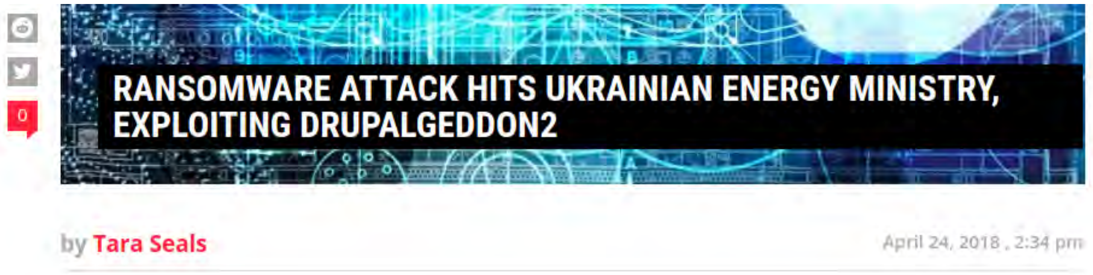
Sophisticated malware attacks through routers

It's likely the creation of a government surveillance agency.

Jon Fingas, @jonfingas
03.11.18 in Security

14 Comments

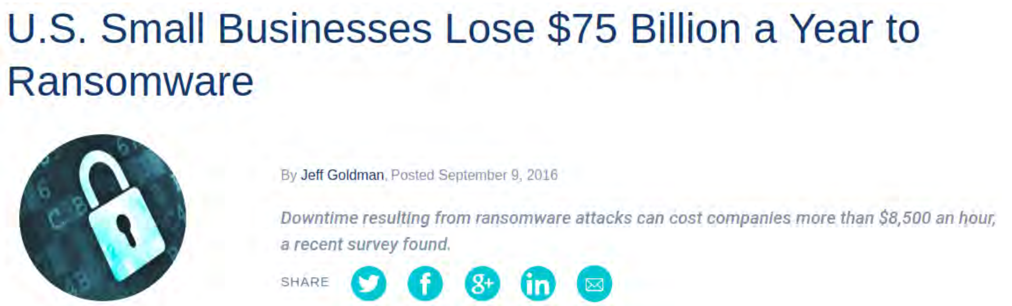
1933 Shares



RANSOMWARE ATTACK HITS UKRAINIAN ENERGY MINISTRY, EXPLOITING DRUPALGEDDON2

by Tara Seals

April 24, 2018 , 2:34 pm

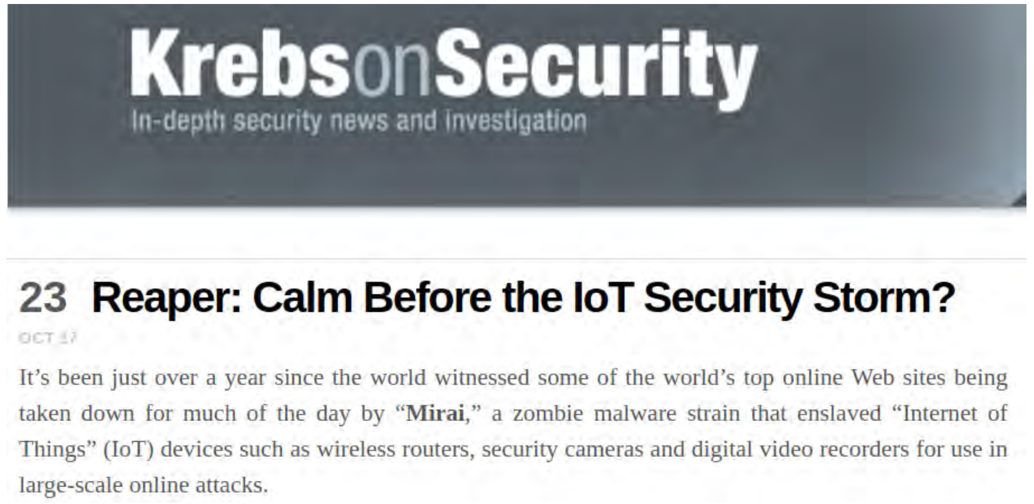


U.S. Small Businesses Lose $75 Billion a Year to Ransomware

By Jeff Goldman, Posted September 9, 2016

Downtime resulting from ransomware attacks can cost companies more than $8,500 an hour, a recent survey found.

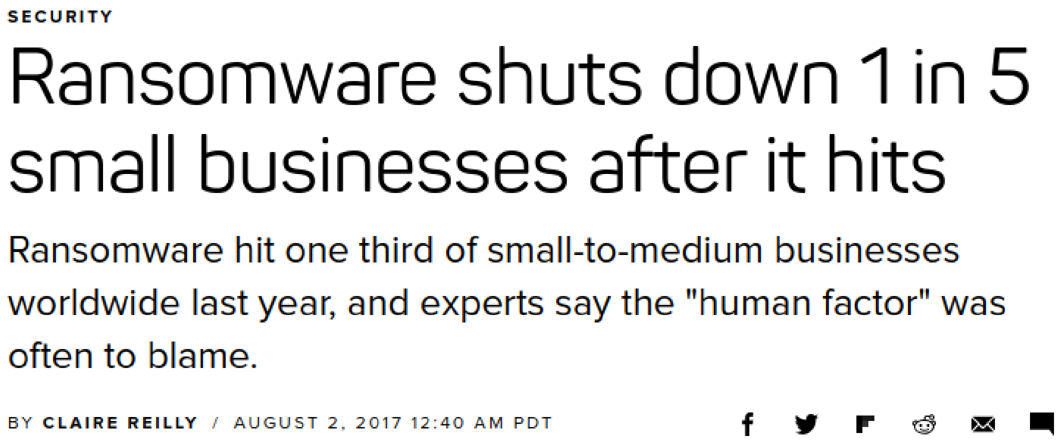
SHARE



23 OCT 17

Reaper: Calm Before the IoT Security Storm?

It's been just over a year since the world witnessed some of the world's top online Web sites being taken down for much of the day by "**Mirai**," a zombie malware strain that enslaved "Internet of Things" (IoT) devices such as wireless routers, security cameras and digital video recorders for use in large-scale online attacks.



SECURITY

Ransomware shuts down 1 in 5 small businesses after it hits

Ransomware hit one third of small-to-medium businesses worldwide last year, and experts say the "human factor" was often to blame.

BY CLAIRE REILLY / AUGUST 2, 2017 12:40 AM PDT

THE PROBLEM

IoT devices are everywhere and not protected

THE PROBLEM

Cybersecurity technology is expensive for home users and small businesses

TANIUM™

paloalto NETWORKS

ArcSight™ An HP Company

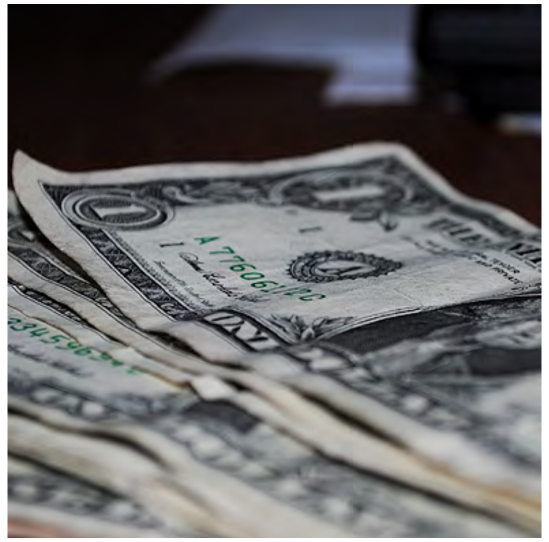
splunk>®

CROWDSTRIKE

QRadar®

THE CHALLENGE

A device that protects people's networks against cyber threats

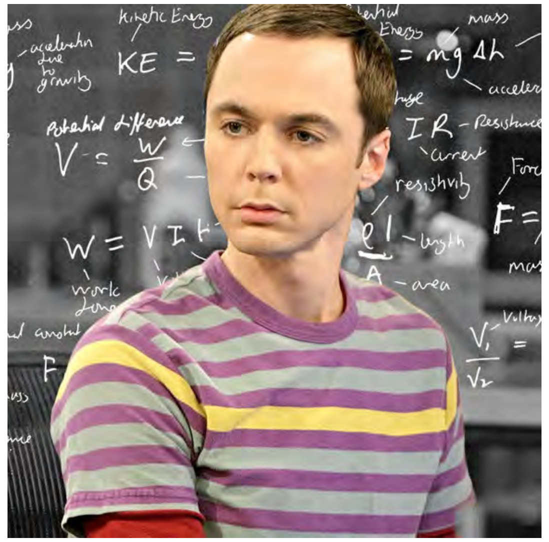


CHEAP

EASY

SMALL

SMART



THE IDEA

THE IDEA

A device that protects people's networks against cyber threats

RASPBERRY PI

> Small and powerful

> Cheap

> Popular (over 19 million RPis sold)

BRO IDS

> Smart

> Lightweight

> Open source

CUSTOM PYTHON CODE

> Versatile

> Popular among developers

THE OUTCOME

Bro IDS

- > Network traffic analysis
- > Metadata extraction

Core Python app

- > Advanced correlation and traffic statistics
- > Alerting
- > Gluing all the stuff together

Dnscrypt-proxy

- > DNS traffic encryption
- > Prevent DNS disclosure

NGINX

- > Admin web console

THC Hydra

- > Detect vulnerable accounts

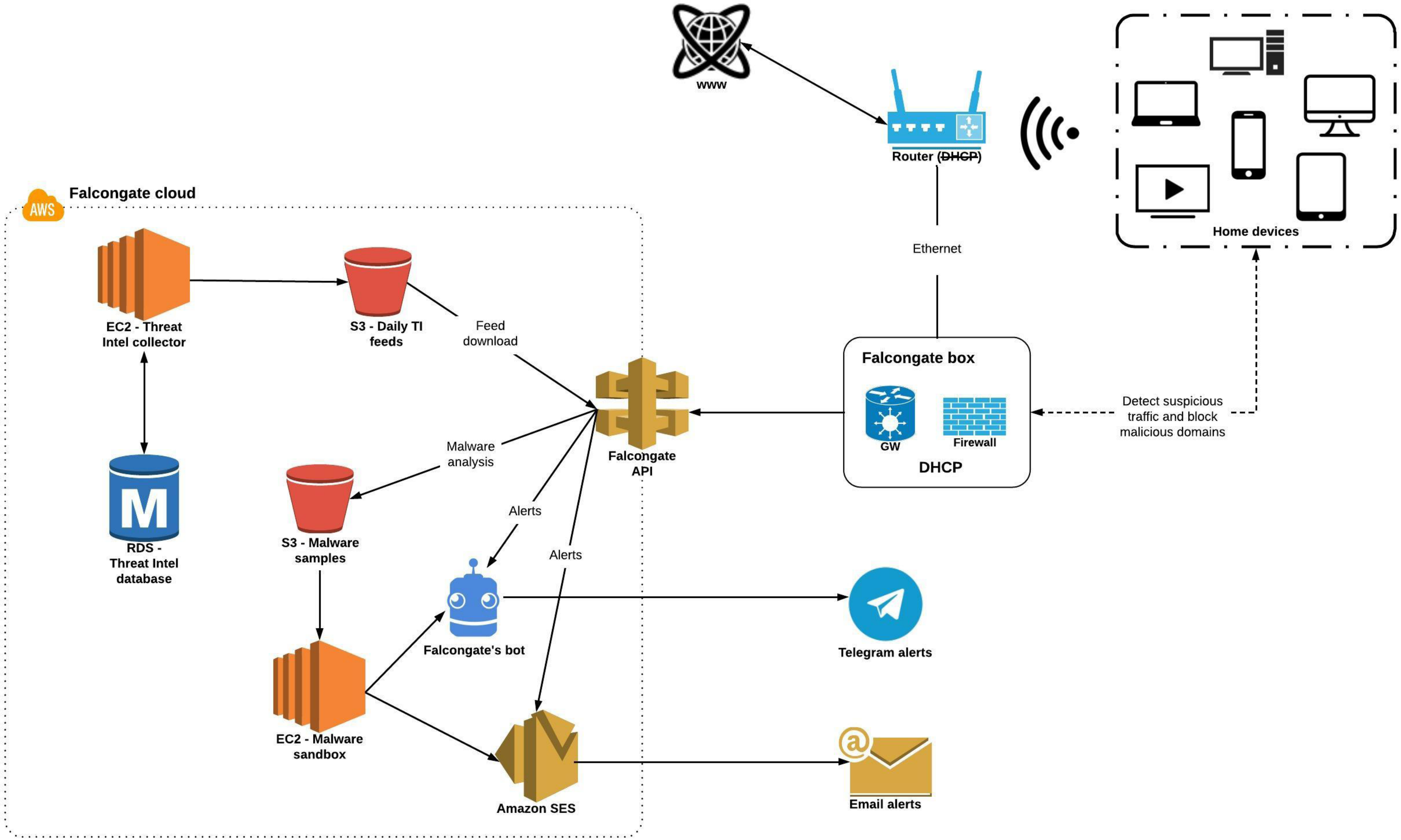
Open Source Intelligence

- > Malicious IP and domain feeds
- > Default passwords feed

Nmap

- > Port discovery

FALCONGATE PLATFORM OVERVIEW



CURRENT FEATURES

- Pro-actively blocks known malware based on our free Threat Intelligence feeds.
- Blocks malware using the Tor network (can be disabled).
- Detects active malware based on existing VirusTotal reports.
- Detects well-known malware traffic patterns like DGA and spamming.
- Detects network intrusion patterns like port scanning and tracerouting.
- Detects and alerts on the presence of vulnerable default vendor accounts in any device in the network.
- Encrypts all your DNS traffic to protect all the devices against DNS spoofing and stops ISPs from spying on your DNS requests.

DEMO

falcongate

https://github.com/A3sal0n/FalconGate

@FalconGate_GW

https://www.facebook.com/falcongate.gw

info@falcongate.cz

THE FUTURE

- Use of Machine Learning models for anomaly detection.
- Additional network statistics and data visualizations in the admin web console.
- Additional heuristic rules for threat detection.
- Improved alerting.
- Apply for funding to develop further the platform:
  - Develop a custom board for the device
  - Develop a custom case
  - Dedicated iOS/Android app for the user console
  - Connect additional Threat Intel sources
  - And much more..

falcongate

By
Leonardo Mokarzel Falcon
& Michal Meravy

GET IN TOUCH

DOWNLOAD THIS PRESENTATION NOW

https://github.com/A3sal0n/FalconGate

https://www.facebook.com/falcongate.gw

@FalconGate_GW

info@falcongate.cz