FREE Live Webinar

Top 5 best practices for cellular IoT device security

Please wait until guests have joined the webinar

EMnify

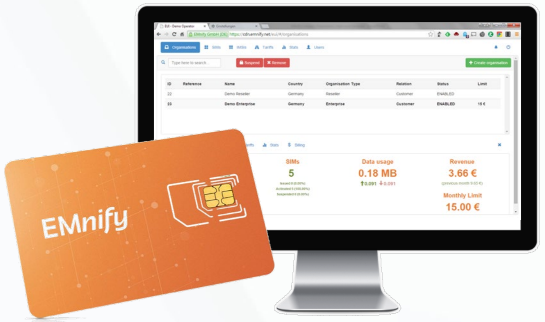
Agenda

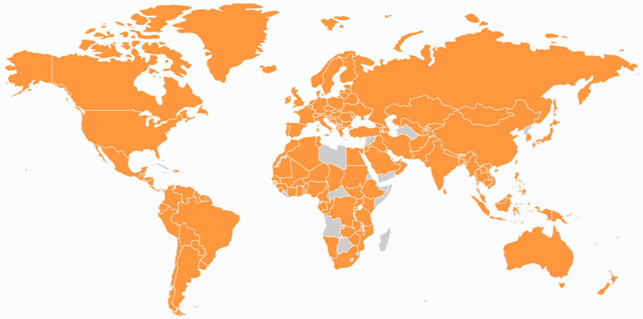
- EMnify Introduction
- Attacker Types and Motivation
- Top 5 Security features
- Q&A

EMnify

Cellular Connectivity
Anywhere In The World

(2G, 3G, 4G, LTE-M, soon NB-IoT)





movistar · T · · · airtel · verizon · O2 · vodafone · 中国移动通信 CHINA MOBILE

VimpelCom · Claro · A1 Telekom Austria Group · telenor group · Telia · WIND · 3 · orange

180+ countries

540+ networks

We are where you are
In the Cloud

aws Azure Google Cloud

devicepilot Keen DATADOG salesforce

Global Distributed

Intra-Cloud Peering for Device Remote Access

Connectivity Meta-Data delivered to Cloud Service

Reliable and Secure Infrastructure

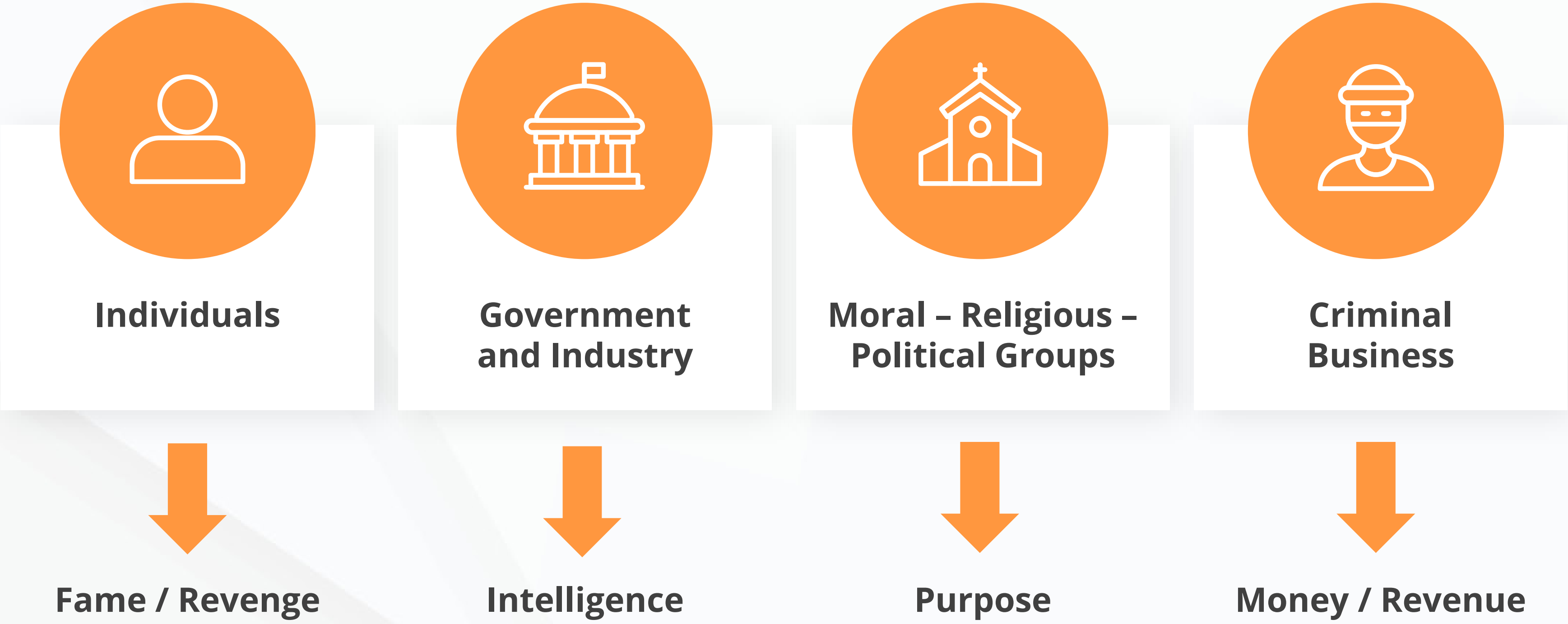
Our Customers – IoT Solutions

Smart Home	Smart City	Health	Retail	Agriculture
Alarm & Surveillance Pest Control Smart Metering Leak Detection	Parking Meter Traffic Control Waste Management Public Safety	Fall Detection Health Monitoring Remote Diagnosis Medication Mgmt	Inventory Mgmt Payment (PoS) Digital store Customer Satisfaction	Crop yield & storage Soil/nutrient Fences mon. Livestock surveillance
PRIMAGAZ FUTURA Produkte mit Zukunft CORAL Detection Systems LÖHRER Alarm- und Sicherheitstechnik	EcoWaste VER-MAC digitalparking SONAH	sleepinnov technology micrel Medical Devices PATH MEDICAL Inspiration Healthcare	Eval&GO Alberici Cash Solutions GPD Tecnovision	ARGOTEC Ingeniería nelume stellapps evja

Asset Mmgmt	Manufacturing	Transportation	Environment
Fleet Mgmt Animal tracking Container tracking Good temperature Art & Relic Preservation	Stock inventory Mgmt Predictive Maintenance Safety Monitoring Machine monitoring	Vehicle Diagnostics Connected Car Rail monitoring	Air/water quality Noise Radiation Flooding Solar & Air Energy
Europcar CargoGuard 2hire Innovalinks Tracking & Logistics	SKF BLACKBIRD Smart Data Collection Explosion Power Syrinix Intelligent Pipeline Monitoring	hoots SPORT TRAXX UBICA móvil Aperia Technologies	campion pumps The power behind water Solarly ATMOTRACK

- B2B2B and B2C
- Selling Connectivity as part of their services

What is the motivation for cybercriminals?



Individuals

Fame / Revenge

Government and Industry

Intelligence

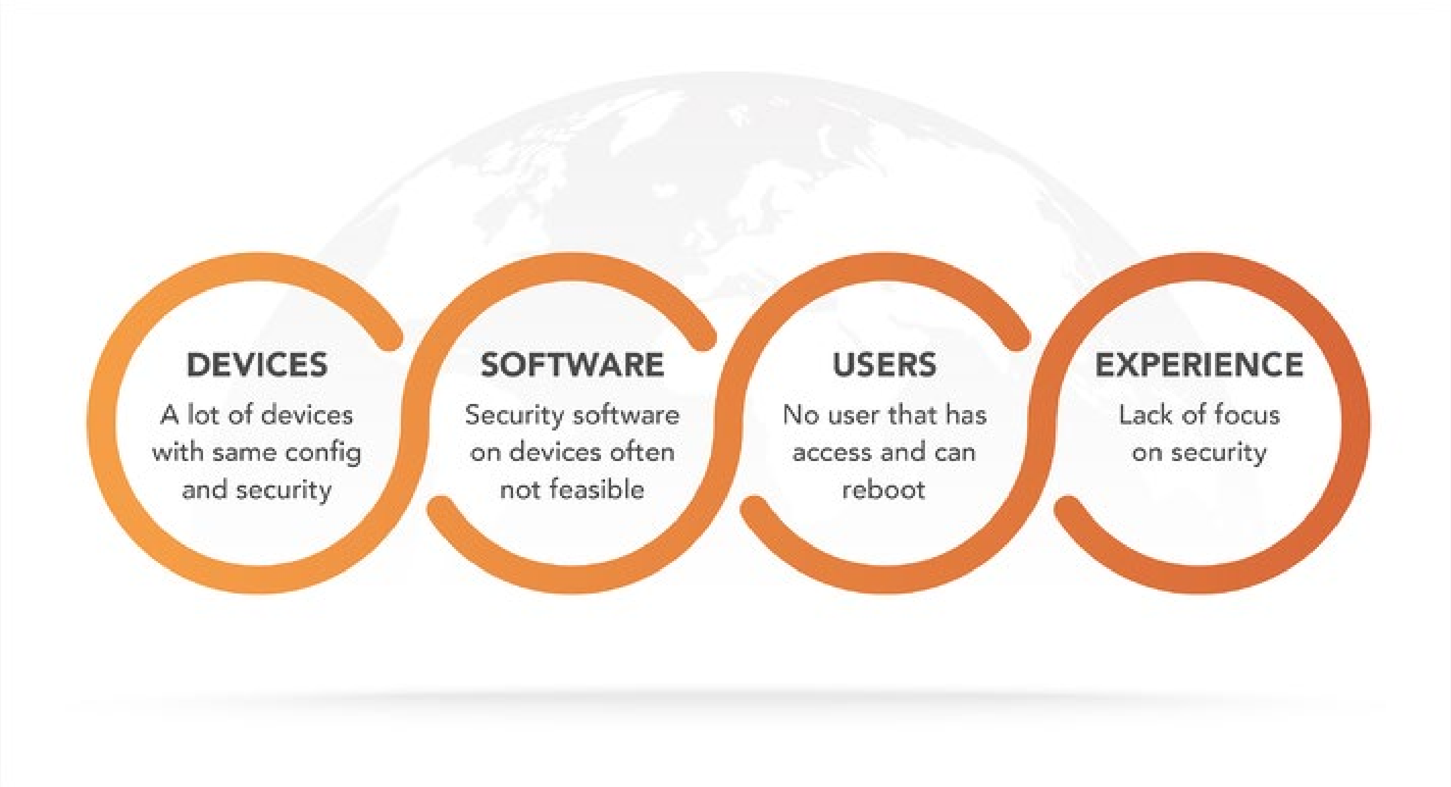
Moral – Religious – Political Groups

Purpose

Criminal Business

Money / Revenue

Why are IoT devices in the **focus of attackers?**



DEVICES
A lot of devices with same config and security

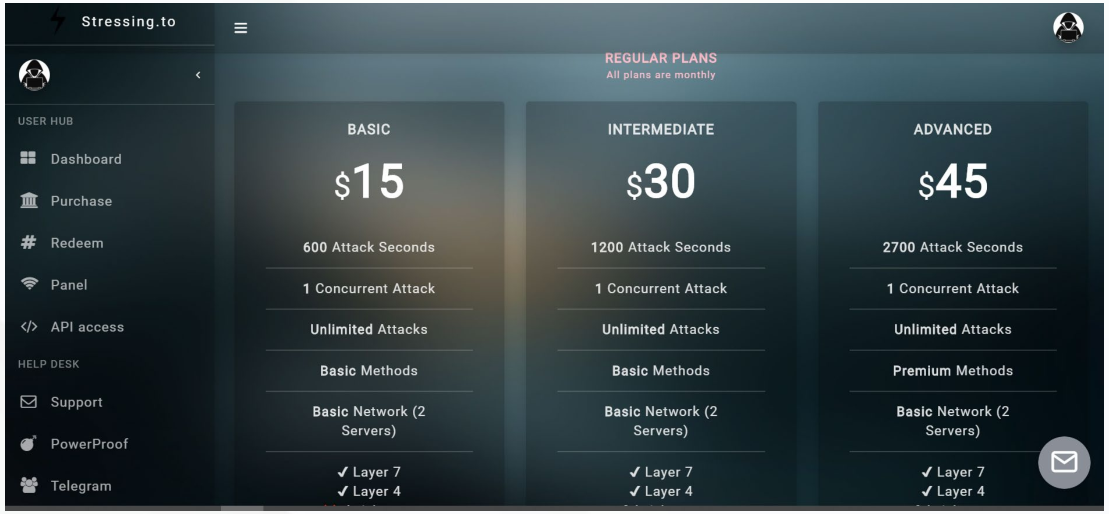
SOFTWARE
Security software on devices often not feasible

USERS
No user that has access and can reboot

EXPERIENCE
Lack of focus on security

How do cybercriminals make money with IoT devices?

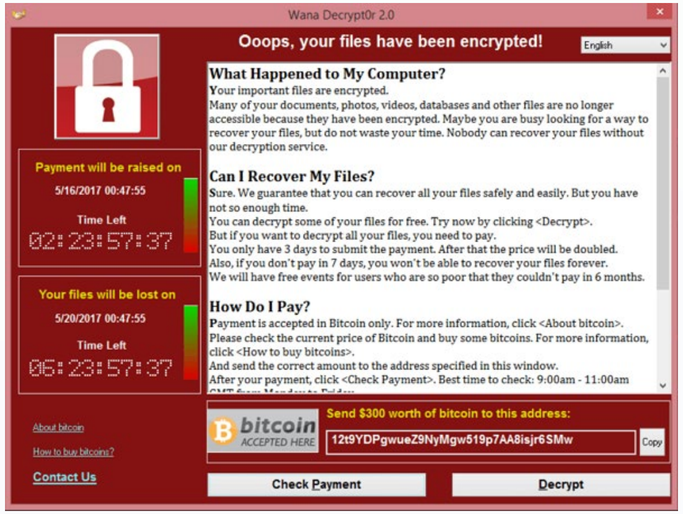
Denial-of-Service Attack as a Service



REGULAR PLANS
All plans are monthly

BASIC	INTERMEDIATE	ADVANCED
$15	$30	$45
600 Attack Seconds	1200 Attack Seconds	2700 Attack Seconds
1 Concurrent Attack	1 Concurrent Attack	1 Concurrent Attack
Unlimited Attacks	Unlimited Attacks	Unlimited Attacks
Basic Methods	Basic Methods	Premium Methods
Basic Network (2 Servers)	Basic Network (2 Servers)	Basic Network (2 Servers)
✓ Layer 7 ✓ Layer 4	✓ Layer 7 ✓ Layer 4	✓ Layer 7 ✓ Layer 4

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

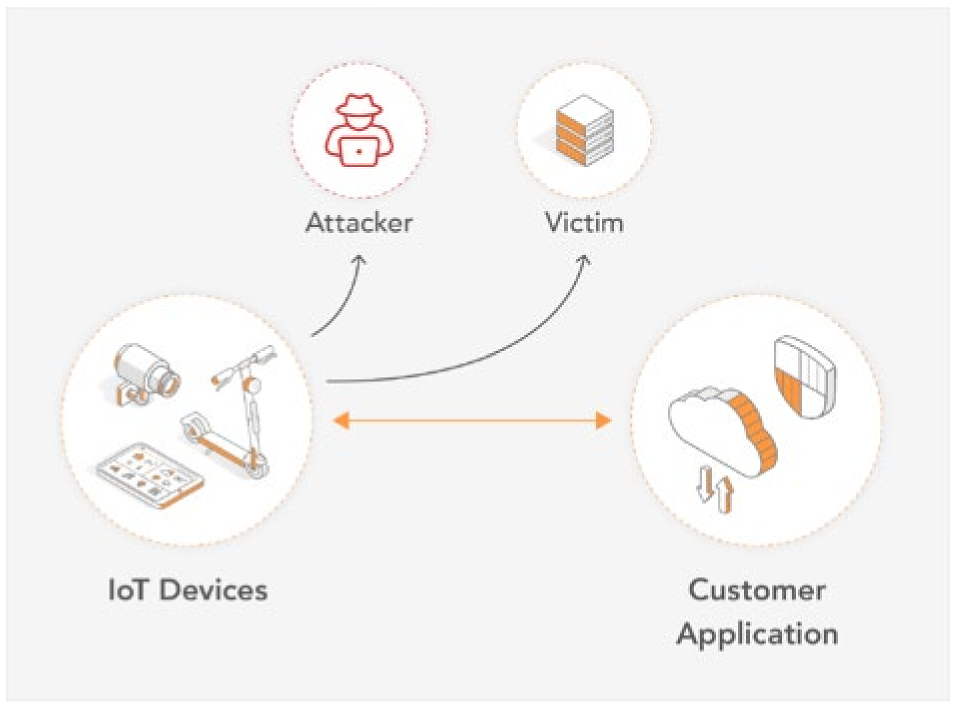
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Crypto Currency Mining
(with less success)

What does a **common IoT attack** look like?



Simplified Mirai attack scheme

Mirai/Chalubo/Liquorbot

- Attackers scan the **public internet** for IoT devices and utilize **remote access** ports to login (using brute force passwords)
- Once control over the device **execute a DDoS attack** on a victim

Stuxnet

- Utilize exploits of windows machines and then spreads to Siemens SCADA PLCs in the **same network –** executing commands on the PLC
- damaged e.g. Iranian atomic program

Brickerbot

- Similar to Mirai – **remote access / public internet** and then making device unusable (brick)

Top 5 cellular features for IoT device security

25+ Best Practices and cellular features to secure IoT devices and applications.

Download here

https://www.emnify.com/guide-for-cellular-iot-security

Top 1: Secure Remote Access

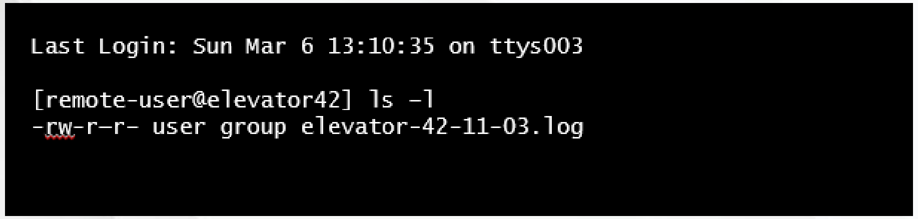
Mirai attack vector: Remote Access via public reachable address

Private / Public IP address of device

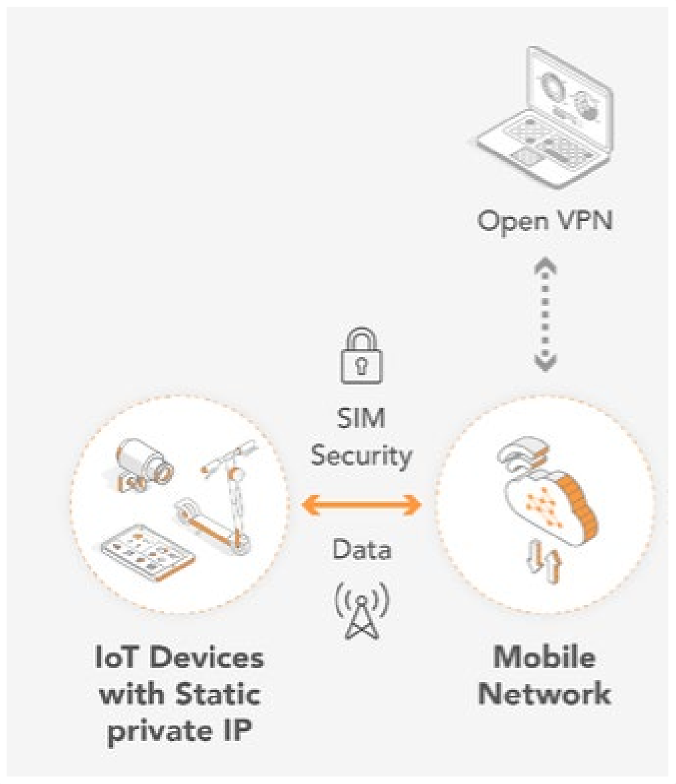
Static / Dynamic IP address

Private IP - takes device off public Internet
Static IP - allows remote access without dynamic DNS service

Remote Access via VPN, by authenticating with cellular connectivity provider to get access to the device



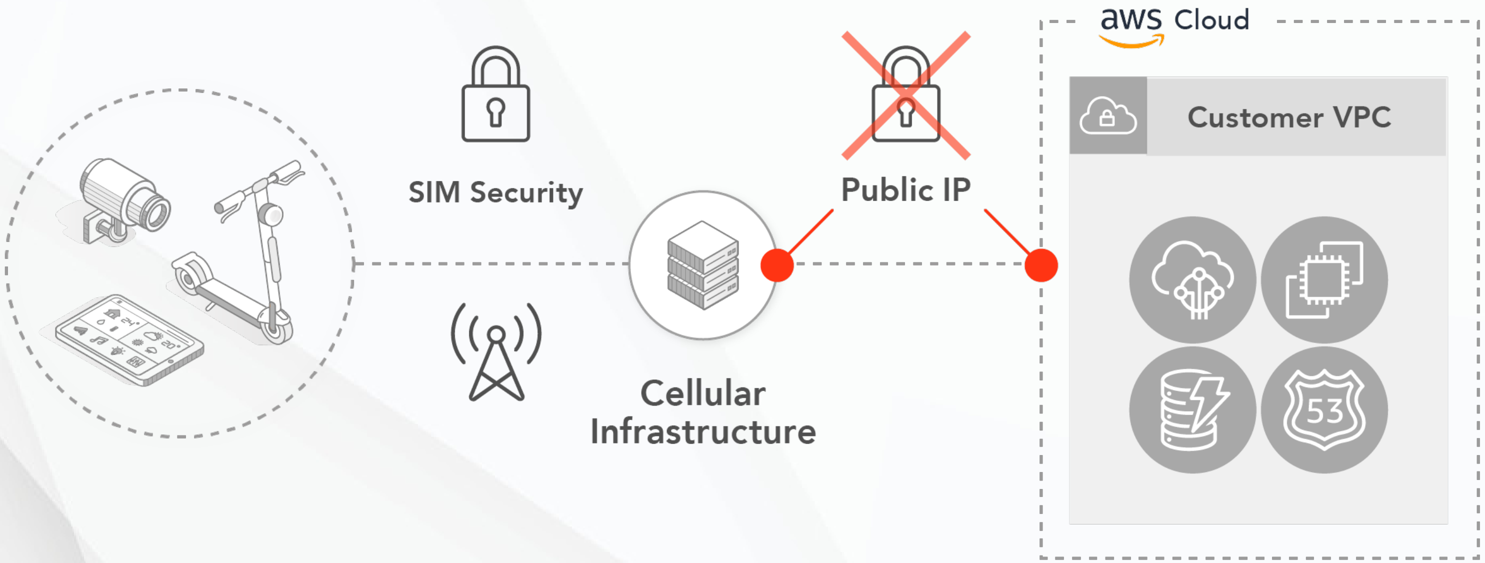
```
Last Login: Sun Mar 6 13:10:35 on ttys003

[remote-user@elevator42] ls -l
-rw-r-r- user group elevator-42-11-03.log
```



- Certificate based authentication
- Private key encryption

Top 2: Closing the Internet Gap

Attack vector: Data Transmission over Public Internet

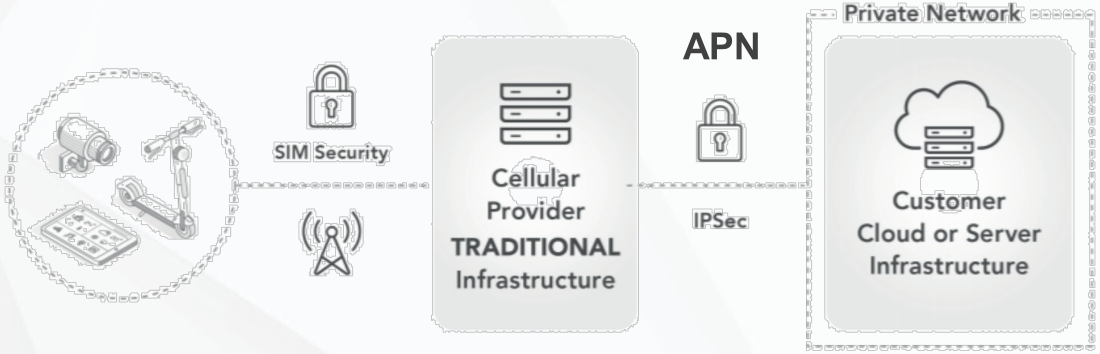


Data secured in the network operator infrastructure using SIM authentication & data encryption

Security Gap – between Mobile network and Application Infrastructure

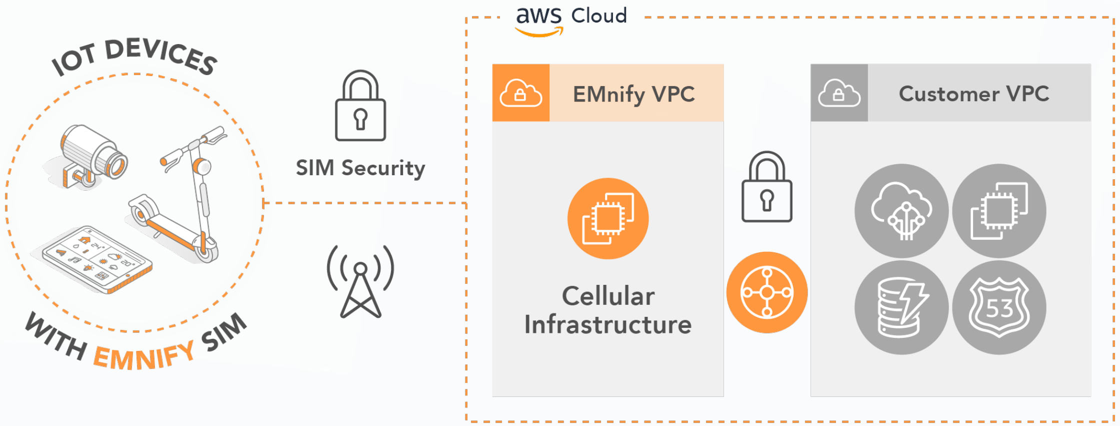
Top 2: Closing the Internet Gap

Traditional - Private APN with IPsec


SIM Security
Cellular Provider TRADITIONAL Infrastructure
APN
IPSec
Private Network
Customer Cloud or Server Infrastructure

- Private APNs - public IP addresses used to establish secure tunnel
- Devices and application can use private IP addresses to communicate (no NAT)
- Data encrypted from infrastructure to cloud
- Secure remote access
- ~x weeks to setup

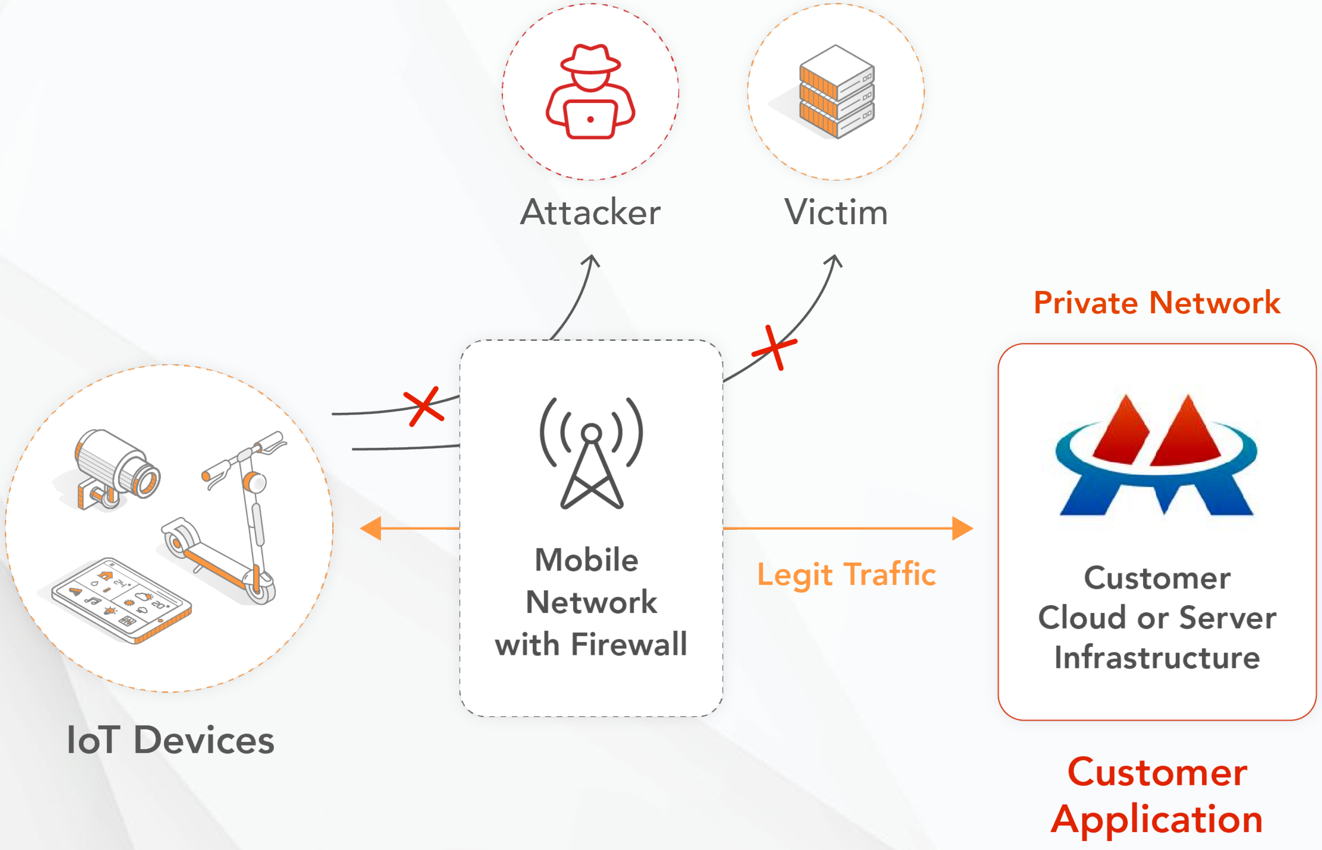
Secure Intra-Cloud Connect



- Intra-cloud connect (no public IPs)
- Setup in minutes
- Complete cloud service model
- Device and application in same VPC – secure data transport and remote access

Top 3: Cellular Data Firewall

Mirai attack vector: Infected Device can be controlled by attacker and attack victim (illegitimate traffic destinations)



Attacker

Victim

Private Network

Mobile Network with Firewall

Legit Traffic

Customer Cloud or Server Infrastructure

IoT Devices

Customer Application

Top 4: Voice and SMS Service Firewall

SMS attacks

Fall 2019
SIMjacker
And
WIB attack

- Use SMS to trigger action on SIM applet (S@T and Wireless Internet Browser)
- Actions: send location, make an SMS, make a call

Voice Fraud

28 billion $ fraud in 2019

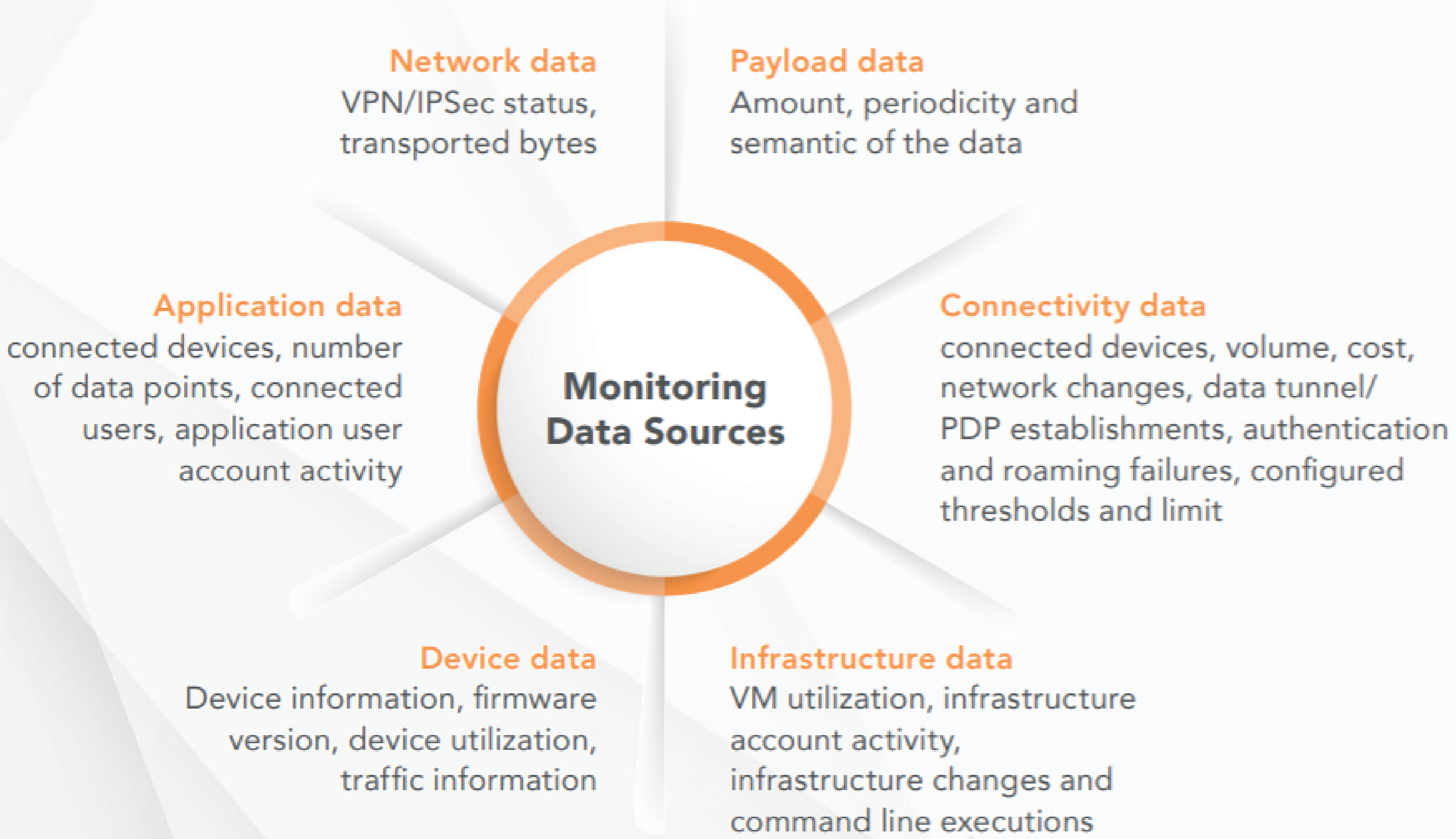
- In case an attacker gets control of devices – via Data, SMS and make premium calls
- International Revenue Shared fraud - company providing the premium number and the one renting sharing revenues

A2P SMS
Internal SMS
MT/MO SMS

ON **OFF**

Voice
External SMS

Top 5: Connectivity Monitoring via Real-Time Datastreamer



Monitoring Data Sources

Network data
VPN/IPSec status, transported bytes

Payload data
Amount, periodicity and semantic of the data

Application data
connected devices, number of data points, connected users, application user account activity

Connectivity data
connected devices, volume, cost, network changes, data tunnel/ PDP establishments, authentication and roaming failures, configured thresholds and limit

Device data
Device information, firmware version, device utilization, traffic information

Infrastructure data
VM utilization, infrastructure account activity, infrastructure changes and command line executions

- Connectivity Data needs to be part of anomaly detection – requires 360° view on system
- User Error vs. Attack
- Real-Time requirements
- Operational Service Dashboard

Summary:

Cellular Security Benefits

Cellular is a separate network (Stuxnet)

Prevents Mirai attacks - Remote access, Closing the gap, Firewall

Own private network between all devices and applications

Central Control of connectivity security per device or group

Central Monitoring for anomaly detection

25+ Best Practices and cellular features to secure IoT devices and applications. With utilizing cellular connectivity features – the most common IoT attacks are prevented.

Download here

https://www.emnify.com/guide-for-cellular-iot-security

Thank you. Q&A

EMnify