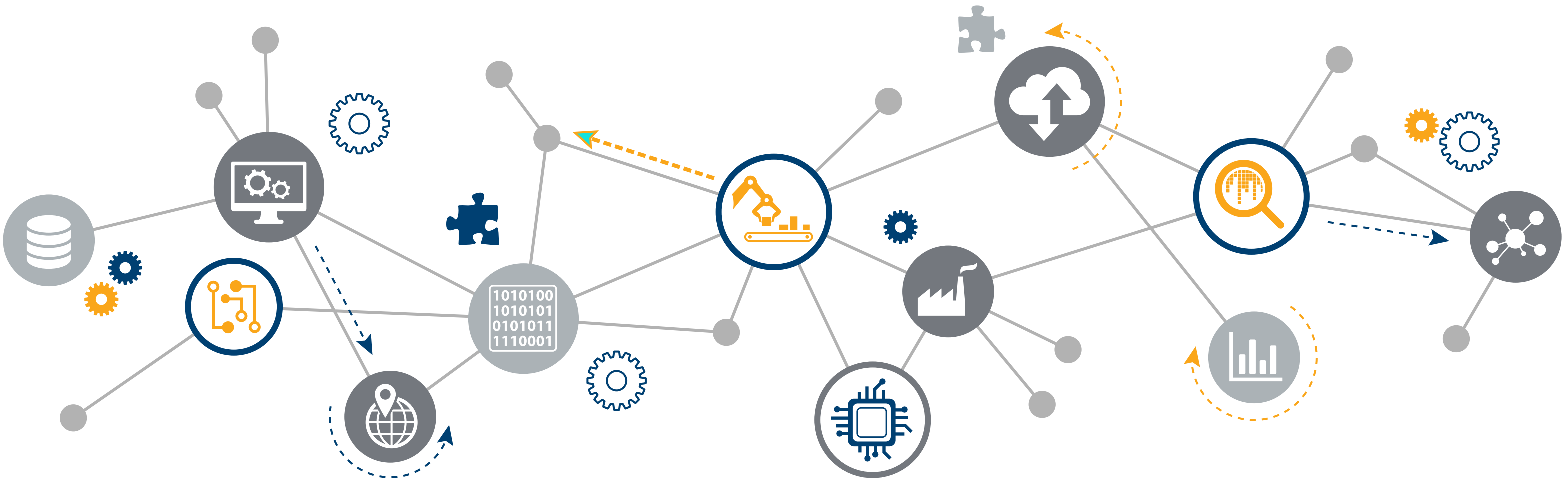
Public

IoT Cyber Security

Analysing Carrier Scale IoT Traffic and Detecting Cyber Threats

April 2019



telesoft-technologies.com

Synopsis

The rate of IoT device global deployment continues to accelerate, with investment in IoT predicted to be over $1 Trillion US by 2020, resulting in many tens of billions of connected devices (source International Data Corporation). By 2025, McKinsey forecasts IoT to generate between $4 and $11 Trillion US of global economic value.

Commercial gains and new sources of revenue drive IoT deployment throughout many industries and sectors, but lack of cyber security regulation and implementation can lead devices to be used for nefarious activity. Gartner [4] predicts that by 2020, 25% of all enterprise attacks will involve IoT devices circumventing the boundaries of traditional network security, combined with a sudden rise in new types of attack vectors.

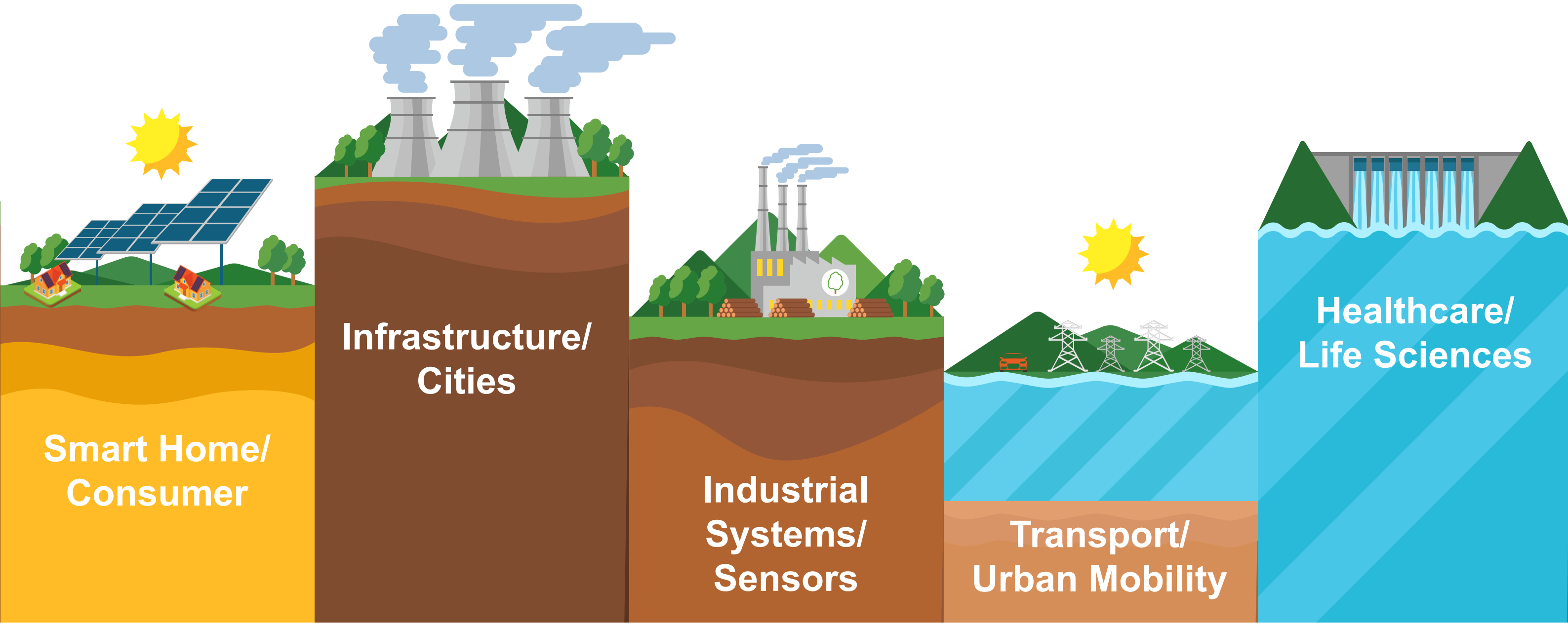
The purpose of this whitepaper is to examine the current state of IoT device security, the resulting impact on large carrier scale networks and the tools and techniques available to detect and mitigate compromised IoT devices.

What is IoT

'Internet of Things' or 'IoT' is an umbrella term for describing a wide range of interconnected, often autonomous devices that exist within the digital world – including:

- Smart cities and municipal services
- Medical devices
- Computing peripherals
- Manufacturing and industrial control systems
- Autonomous cars, ships and traffic management
- Home devices white goods, locks, energy control, media and AI assistants
- Consumables such as wearable technology and toys
- Land management including irrigation, lighting feed control and agriculture
- Construction and buildings management

Benefits driving adoption include more intelligent, efficient and responsive commercial business operations, enhanced lifestyles and efficient households.



We can categorise IoT devices into three groups:

1. Devices that collect then send information
2. Devices that receive and act on information
3. Devices that can do both

IoT deployments can mix short range communication including WiFi, NFC, ZigBee, Z-Wave, RFID and Bluetooth, often used for remote sensors, with wider area communication providing internet access to applications and data processing over LoRa, NB-IoT, 3G, 4G and GSM LTE [7]. This access makes devices vulnerable to attackers.

Security Risks Linked to IoT

From a carrier perspective, malicious activity executed by large numbers of compromised IoT devices can be seen within the subscriber data content (the user plane) and the network signalling (the control plane). This affects service delivery and is a potential source for loss of revenue through fraudulent use of the network, infrastructure or services.

Impact occurs regardless of intent. Normal behaviour of IoT devices may have unintended detrimental consequences for the carrier. These include increased signalling load on the core network infrastructure and services, large amounts of devices communicating information, and reductions in QoS (Quality of Service) for other subscribers.

Many IoT devices have little or no on-board security, widening the attack surface to insecure and vulnerable communication protocols such as UPnP (Universal Plug ‘n’ Play). Akamai Technologies found 4.1 million internet facing UPnP devices being employed in DDoS attacks [9]. Even when vulnerabilities are identified in IoT devices, it is often difficult to apply security patches, either due to their location, prohibitive cost, poor design or limited technical expertise of the owner leaving devices open to compromise extended periods of time.

Very little consensus in the form of legislation and standards exist for IoT device security. This is typified in the United States, where a number of pieces of legislation have been proposed but only the SB-327 bill, “Security of Connected Devices” in the state of California has been passed into law. This has been criticised for being vague with a focus on adding good security features rather than removing bad ones.

Attack Attribution and IoT

A particular problem occurs in networks that use NAT (Network Address Translation), a method that remaps one IP address space into another to conserve expensive or limited public IPv4 addresses. This normally takes place within a dedicated device or is a function on a router/switch/firewall/gateway. NATing takes place in many networks but notably at extremely high rates in telecommunications operators, high performance computing and data centres, multi-site large organisations and other distributed networks with public internet access via a gateway.

This makes it difficult to attribute behaviour to a device or subscriber account when using the public IP address. In practical terms this means that without cross-NAT attribution it is impossible to trace a threat or attack during incident forensics starting from a public or NATted IP address.

Botnets

Botnets are groups of compromised devices, or zombies, controlled by a bad entity commonly known as a herder. "Command and control" messages, better known as C2 or CnC, allow the herder to control botnet activity either via C2 servers or peer-to-peer communications.

Uses of botnets are continually evolving but include:

- Distributed Denial of Service (DDoS) attacks
- Crimeware, malware and ransomware distribution
- Cryptojacking
- Marketing fraud including CPC (cost per click)
- Intelligence gathering and target profiling

Attacks originating from botnets form a significant proportion of those launched on a carrier network. Especially as the number of carrier networks capable of monitoring and alerting on botnet activity grows, the faster and more decisive the collective and distributed response becomes against the IoT based botnet threat.

Harvesting is a term used when growing a botnet larger. The large numbers of deployed IoT devices with limited security capabilities make them ideal for use in bulk harvesting, whilst also providing a low technical barrier to engage in this practice.

One of the first botnets to autonomously harvest IoT devices was Mirai in 2016, released via code-sharing site Github. This botnet exploited the Telnet protocol and was a significant contributor to the 600% rise in IoT DDoS attacks seen in 2016-17.

In contrary to Mirai, the Hajime botnet (which means 'Beginning' in Japanese) uses similar techniques to hijack IoT devices then secure the device from being taken over by other botnets by blocking ports such as '23', '7547', '5358 and '5555' which are all common entry points for attack vectors like Mirai, QBot and other threats. Once the device is infected by Hajime it remains dormant and carries out no (currently known) further malicious activity.

Command and Control (C2, CnC)

Identification, classification and disruption of botnet C2 is a critical element of carrier security tools. Some of the same security vulnerabilities such as the use of HTTP rather than HTTPS or Telnet rather than SSH, enables a device to be compromised also simplify mapping, profiling and mitigation of botnets.

To detect and respond to botnets in a carrier scale environment, security operations teams need access to:

- Network flow metadata collection and enrichment for full network visibility
- DPI and signature matching (such as IDS tools: Suricata, Snort and Bro)
- DNS analysis and behavioural analytics
- Up-to-date threat intelligence

As botnet capabilities cover both bulk network activity (such as DDoS) and single-flow threats (such as malware delivery) there is a need for full network activity visibility, using tools that work on a per-flow granularity at the multi Terabits per second found on carrier networks. These tools also need to operate in near real-time for incident alerting and response so that threats can be mitigated in a sufficient timeframe.

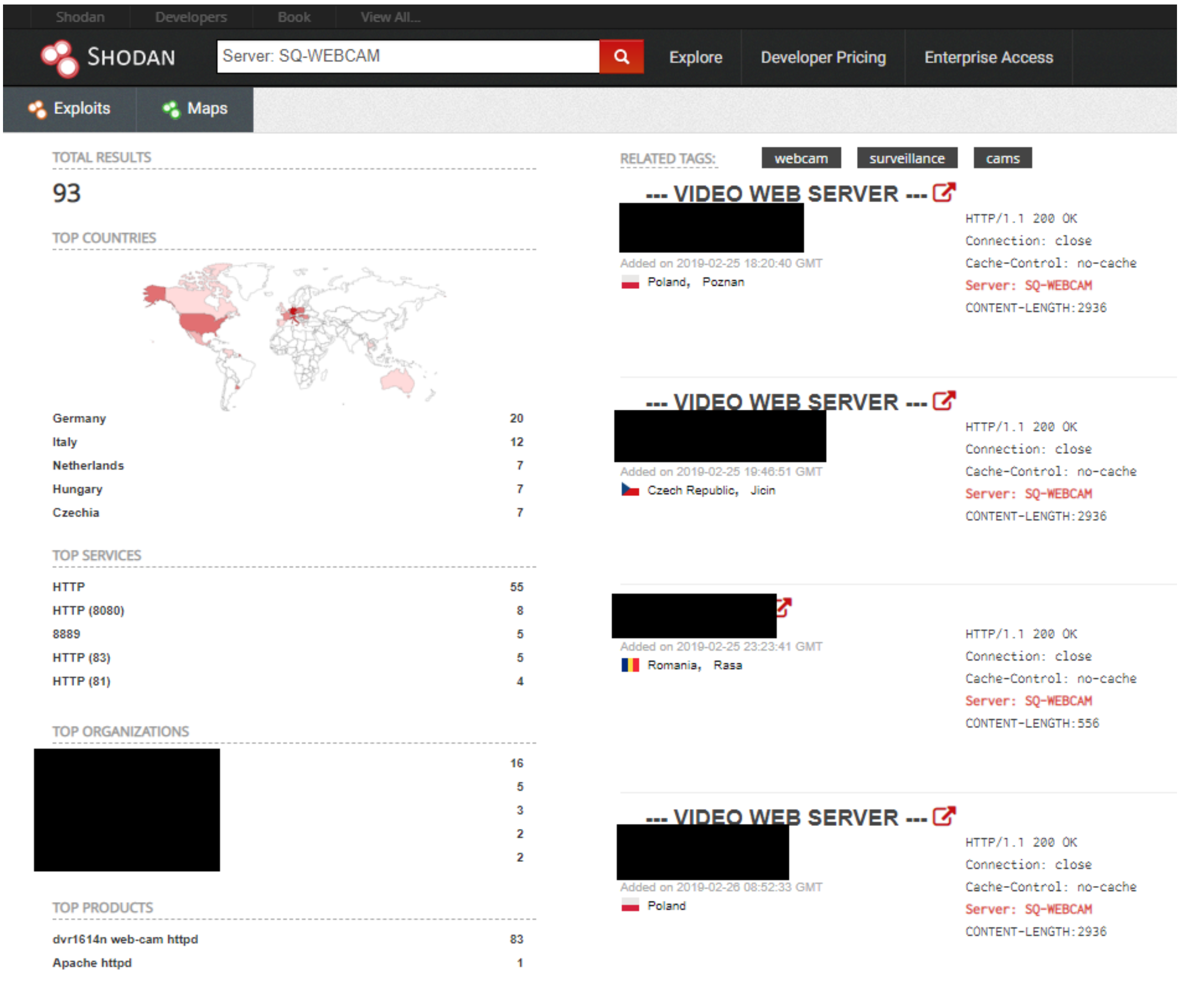
IoT Botnet Target Reconnaissance & Intelligence

There are two victims of IoT Botnet attacks, the actual botnet target and also the individual IoT device owner, who are usually consumers participating in cyber-attacks without their knowledge.

Mass harvesting of IoT devices can be done using various techniques including:

- Google dork searching
- IoT search engines (Shodan)
- Botnet spreading methods
- IoT manufacturer cloud services (Discover)

These techniques allow attackers to locate the online devices and execute vulnerabilities or brute force weak authentication allowing them to control the device. IoT targeting and recon can be executed with little difficulty with the help of IoT search engines, such as Shodan, which are readily available for both attackers and defenders. These tools can highlight the enormous number of insecure devices available, for example upon searching for devices such as webcams Shodan provides a list of devices tagged with 'webcam' and lists the vulnerabilities associated with each device.



Server: SQ-WEBCAM

TOTAL RESULTS

93

TOP COUNTRIES

Germany	20
Italy	12
Netherlands	7
Hungary	7
Czechia	7

TOP SERVICES

HTTP	55
HTTP (8080)	8
8889	5
HTTP (83)	5
HTTP (81)	4

TOP ORGANIZATIONS

[redacted]	16
	5
	3
	2
	2

TOP PRODUCTS

dvr1614n web-cam httpd	83
Apache httpd	1

RELATED TAGS: webcam surveillance cams

--- VIDEO WEB SERVER ---

[redacted]

Added on 2019-02-25 18:20:40 GMT

Poland, Poznan

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2936
```

--- VIDEO WEB SERVER ---

[redacted]

Added on 2019-02-25 19:46:51 GMT

Czech Republic, Jicin

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2936
```

[redacted]

Added on 2019-02-25 23:23:41 GMT

Romania, Rasa

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:556
```

--- VIDEO WEB SERVER ---

[redacted]

Added on 2019-02-26 08:52:33 GMT

Poland

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2936
```

Figure1 – Shodan search query

Attackers can create scripts to harvest an array of devices that meet a tagged criteria and collate them into a list to perform an attacks using potential vulnerabilities.

Impact of Mesh Topology

IoT devices have the ability to work together in a mesh topology, allowing them to autonomously share information to provide faster, more accurate and more resilient services to their consumers. However, with an increasing number of IoT devices and communication between them it raises the question: How is this impacting carrier networks?

Mesh communication between IoT devices, statistics reporting or bulk device software updates could be mistaken as botnet activity. Carriers will need fully unsampled visibility of their network along with threat intelligence if they wish to effectively protect their networks from real threats.

IoT Attack Case Study

One of the most common IoT Botnets attacks is a denial of service. The following describe an IoT Botnet attacking a webserver on an enterprise network and available mitigation techniques.

Figure 2 shows IoT devices 'Zombies/Bots' in a swarming methodology. The herder appoints a target and the method of attack supported by the botnet software (SYN Flood, UDP Flood, DNS amplification, etc.) and then initiates the attack. The network attempts to deliver data packets to the destination, however in this scenario there is no security in place to identify and alert defenders that this traffic as out of ordinary i.e. an indicators of an attack or anomaly.

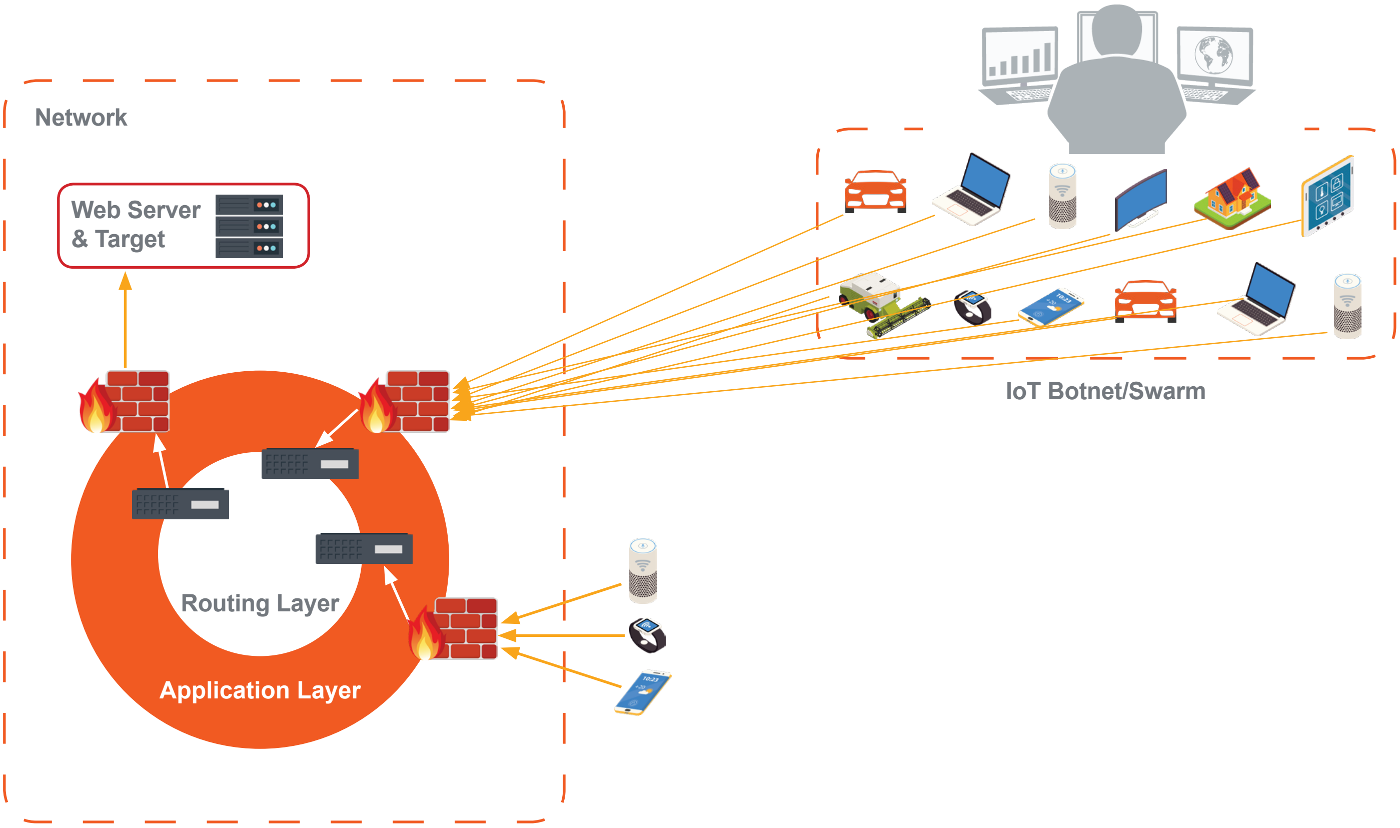


Figure 2 – IoT Botnet attack scenario

UDP flood is a type of DDoS where the attacker attempts to overwhelm ports of a target host by sending IP packets containing UDP datagrams. The target receives the datagrams and sends back a reply "Destination Unreachable", the more UDP packets that are sent and replied the more overwhelmed the target becomes eventually returning an unavailable message for other clients. There are many variants of UDP flood attacks, including spoofing the return address to direct the 'Destination Unreachable' elsewhere to overwhelm another destination.

Mobile Network Core Signalling Disruption

Signalling disruptions within an LTE network are not always malicious and can sometimes be caused unintentionally. As more LTE/5G connected IoT devices enter the market we can expect to see these incidents increase.

Intentional signalling storms are malicious attacks which disrupt the signalling within the LTE core network. Disruption may not always be the primary objective of an attack but rather a side-effect of the attack method. For example, a botnet compromised of LTE connected IoT devices conducting a DDoS attack would need to perform standard tunnel setup (steps within the LTE core) which includes S1AP/S11/S1-MME/GTP-C procedures. The typical nature of DDoS attacks is to open multiple connections in rapid succession to overwhelm their target. The side effect of this within an LTE network is that it can cause signalling plane saturation and result in disruption to the signalling within the LTE core network.

One example of an unintentional signalling storm is the mass communication of IoT devices. Usual network traffic trends and peaks can be predicted, for example during commuter rush-hour and public events. But IoT device mesh communication or software updates is harder to forecast. A software update released for a large deployment of IoT devices could result in a large unexpected surge in activity, with each device needing to setup connectivity involving S1AP/S11/S1-MME/GTP-C signalling. This activity could saturate parts of the LTE network and may appear to security specialist as an attack.

Being able to monitor and decode multiple signalling and data plane interfaces across virtual, physical, cloud and NFV infrastructure is becoming increasingly important to effectively identify what is malicious and what is accidental. In LTE, signalling/Control Plane decode including S1-AP, GTP-C/U and RADIUS/DIAMETER is normalised and stitched to User Plane flow records, often the de-tunnelled GTP-U traffic on the S5/S8 traffic on the S1-U and/or SGi. Both Control and User Plane traffic is then passed through anomaly detection and behavioural analytics, allowing a network provider to determine if a surge in traffic is malicious and if so rapidly apply blocking to mitigate an attack, or if accidental (such as a manufacture device update) apply throttling to prevent network saturation.

Mitigating IoT-based Attacks

Accuracy is essential in automated threat detection and mitigation to avoid disruption of legitimate customer traffic and services. Automated mitigation enables instantaneous response to attacks and removes potential human error. Figure 3 shows a mitigation scenario against UDP flood and Single flow attack.

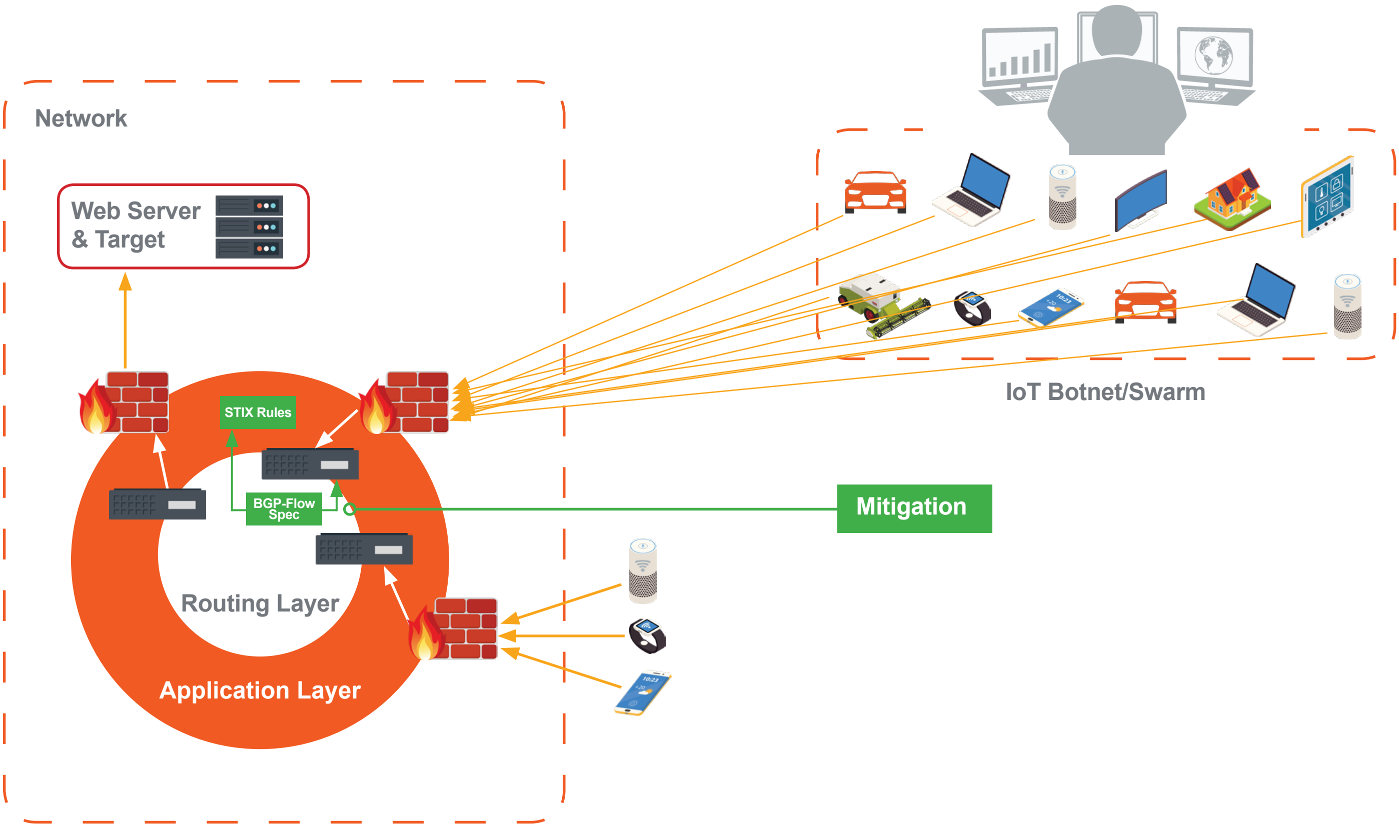


Figure 3 – Attack scenario with mitigation implemented

Anomaly detection and strategic decision-making algorithms can identify single and bulk-flow threat traffic, which can be blocked through rules applied to network routing infrastructure.

Traffic Routing with RTBH and BGP-Flow Spec Outline

Once a threat or anomaly is detected, it is verified and information is extracted to apply rules to routers within the network being protected. Remote Trigger Blackhole (RTBH) is a long-established technique to dump all DDoS traffic into a bottomless pit, either by source or destination IP or service. RTBH is an all or nothing method that allows little differentiation between wanted and unwanted traffic [2].

BGP Flowspec is more granular, allowing the creation of instructions that match a specific flow, blocking attacks such as DDoS, without losing wanted traffic unlike RTBH. BGP Flow specifications can include the following:

- Destination and source prefix
- IP protocol
- Source and destination port
- ICMP type and code
- TCP flags
- Packet length
- DSCP
- Fragment encoding

IoT-based Attack Mitigation at Carrier Scale

Threat mitigation techniques in carrier networks differ from enterprise where the aim is to protect the business from all threats. In a carrier network, threat response and mitigation is far more considered, deliberate and policy-driven, with distributed action across the entire network.

Carriers will use any available defensive features built into existing infrastructure such as BGP-FS (Border Gateway Protocol FlowSpec) and OpenFlow to throttle, route and blackhole traffic with coarse rules. These are generally used discerningly as making continual and rapid routing rule changes in the network carries a risk of inadvertent treatment of non-malicious traffic.

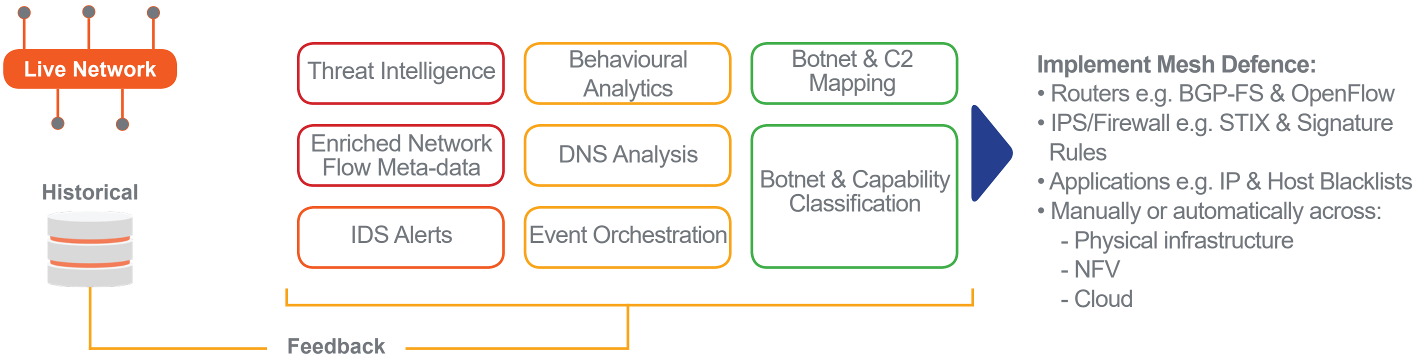
When considering threat detection and mitigation toolsets and platforms, defenders should seek those that utilise BGP-FS or OpenFlow rules which are ideal for DDoS detection when triggered by a target host or IP. The chosen toolset or platform should be able to build relevant BGP-FS/OpenFlow rules and either prompt a human operator to effect the rule throughout the physical, virtual and edge network routing infrastructure or be configured to automatically send the rule out.

If the carrier network infrastructure, customer and service and topology are known (either manually, automatically or through self-discovery), attacks such as DDoS can be blocked for specific entities (customers, physical elements, services).

In LTE networks, two rules may be required to reroute separate User Plane and Control Plane traffic, such as LTE-S1. Here the MME (Mobility Management Entity) needs to be protected from Signalling Storms carried on the S1-MME interface and the SGW (Serving Gateway) needs to be protected from high volume user plane DDoS traffic on the S1-U interface.

When single network flow threats such as crimeware, cryptojacking and SCADA are detected, the toolset and/or platform should notify Security Operations and track the threat through the network infrastructure and services by generating a standardised rule (such used within STIX, Suricata or Snort) for implementation on the host network firewall and Intrusion Prevention Systems.

Collecting accurate and actionable threat intelligence for use by Security Operations and Network Operations teams can be sourced from third parties, open source, peer networks or generated from real-time and forensic analysis of historical data stored in the carriers own cyber platform.



Implement Mesh Defence:
- Routers e.g. BGP-FS & OpenFlow
- IPS/Firewall e.g. STIX & Signature Rules
- Applications e.g. IP & Host Blacklists
- Manually or automatically across:
  - Physical infrastructure
  - NFV
  - Cloud

The diagram above shows typical components of a carrier's cyber platform, and specific features for botnet and botnet swarm mapping. In this scenario, botnet C2 and zombies are continually analysed and network flows to/from compromised devices, enhanced with DNS and host ID collected. This provides current and historical maps of the botnet and a good, simple single filter for forensics and analysis.

Combining this filter with additional real-time behavioural analytics and a feedback loop between the two (allowing the filter to be modified) enables classification of the botnet's purpose such as DDoS, malware, spam, cryptojacking and/or other.

With this information, SecOps can detect botnet activation either by behaviour or by activity of one or more zombies. With the attack capability already known and with network flow (NetFlow/IPFIX) metadata enriched with hosts, DNS, etc.., the Security Operations team can start enforcing one of a number of strategies against the botnet before or within the first few flows of an attack:

- Disrupt the botnet C2, either via network DNS adjustments or peer-to-peer/host blocking
- Throttle and block all known attack vectors in the User Plane, S1/S5/S8/SGi/edge
- Apply throttling and blocking rules in the core network Control Plane, S1/S11/S5/S8

The rules that enforce these changes can be crafted to protect a specific targeted customer, the host network infrastructure and services. Or to enforce the policy/objective of the carrier network with regards to internet traffic i.e. optimally route the attack through the network to the perimeter.

Telesoft's Carrier Scale Security Platform and Tools

Telesoft Technologies provides highly scalable threat detection and visibility tools enabling incident response and forensics in real time, at scale, in carrier physical and NFV networks running at multiples of 100Gbps.

- IoT Probe – 200Gbps core network sensor (telco core compatible)
- vFlowProbe – NFV and on-premises cloud network sensor (5G and edge cloud compatible)
- CERNE – 100Gbps signature matching and "back-in-time buffer"
- FlowStash - data enrichment, streaming analytics and data brokering
- TDAC – ultra scale event orchestration, multi-layered threat detection and mitigation, Petabyte scale distributed storage

The IoT Probe is a network sensor providing visibility for sessions crossing a NAT, attribution to a device/subscriber and network signalling with support for tunnelling and encapsulation.

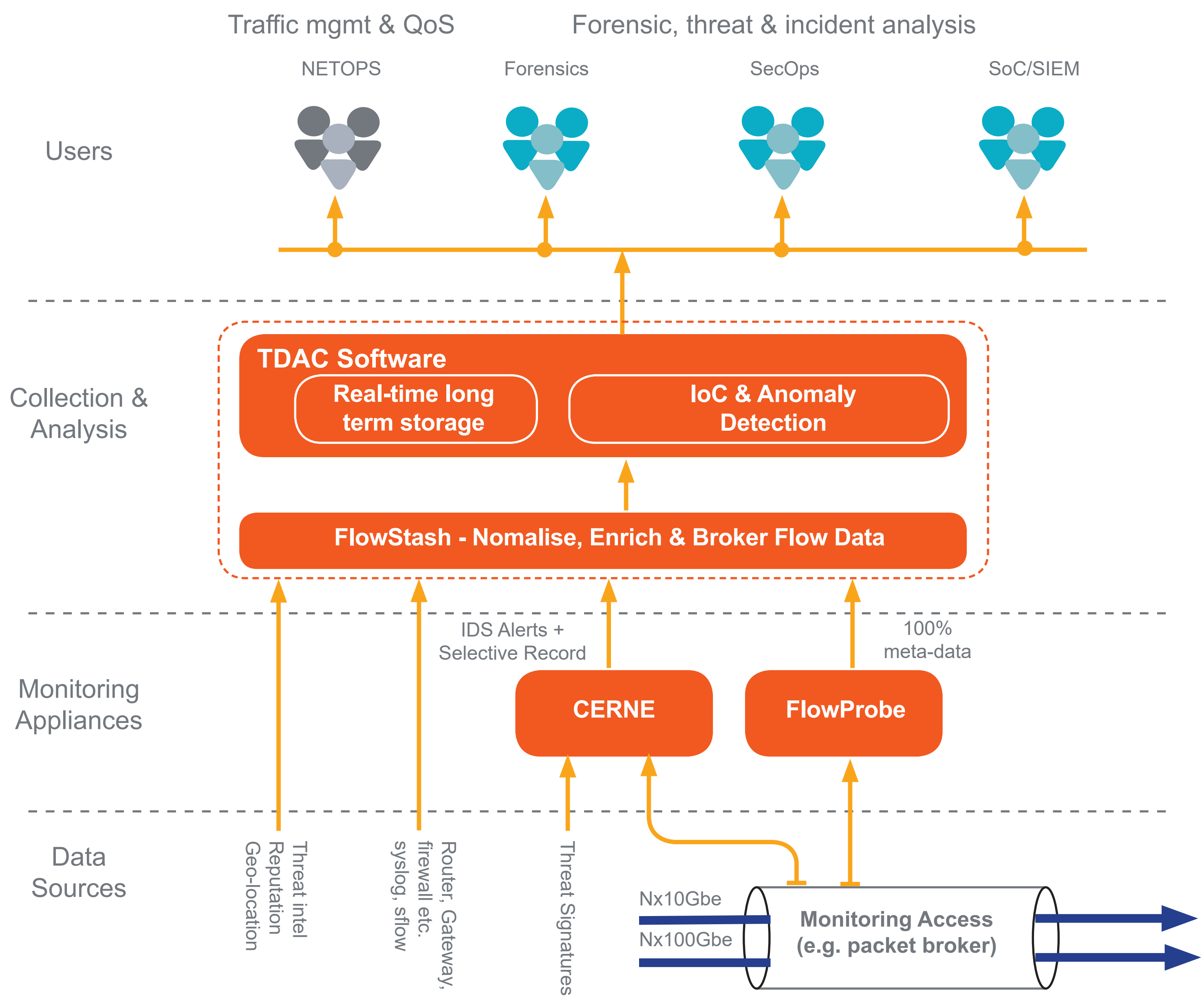
The IPFix is an IETF protocol and was created to universally standardise the export of IP Flows from routers, probes and other network devices. Once egressed by the converter the TDAC can start creating unique dashboards and alert in real-time when an anomaly occurrence happens. By integrating FlowStash (Converter) with PGW (NAT) we can.

The Telesoft CERNE combines a high rate 100Gbps IDS engine based on the Open Source Suricata with automated re-assembly and "back in time buffer" of relevant network traffic for real-time and historical threat investigation. SCADA and IoT threat intelligence rules are available as well as wider IP LAN-based threat intelligence and bespoke intel. The CERNE platform generates signature-based alerts for analysis in TDAC and stores the raw network data as PCAP for subsequent forensic investigations. Should the threat be detected into the flow, the buffer allows going back in time to capture the full network flow from the start – critically maintaining the complete visibility of the incident.

The FlowStash is a scalable high performance platform that transforms, enriches and brokers flow data from numerous physical and logical pieces of the security infrastructure. The Converter consolidates streaming, analysis and classification of network flow meta-data, efficiently pre-processing data for delivery to third party traffic collection and analysis tools. Refer to Figure 4 for a diagram.

TDAC (Telesoft Data Analytics Capability) is a cost effective, field-proven ultra-high-rate monitoring, analytics and forensics platform. TDAC ingests and analyses millions of events per second, including network flow data, IDS alerts and system logs, enhancing data with known threat intelligence (including IP reputation, threat classification, geo-location), partitioning and pre-analysing data for rapid sub-second query by Incident Response and Forensics teams. TDAC can detect attacks and apply targeted rules to existing supporting infrastructure throughout the physical, virtual, routing and application layers within CSP networks to mitigate a wide variety of cyber and revenue threats.

Telesoft Carrier Scale Monitoring and Visibility Infrastructure Integration



Summary

The growth in the number and scale of IoT device deployments is extremely rapid and with the wide number commercial, personal and military applications this growth is set to continue to rise at an exponential pace for the foreseeable future. Devices are easily compromised with a low technical barrier and openly-available tools for any suitably-motivated individual or group. As the digital world evolves to 5G and this becomes a dominant technology the number of IoT devices, and subscribers, will transfer to using telecoms networks for all their connectivity – adding significant revenue opportunity for communications providers. This revenue opportunity is accompanied by a significant increase in scale of data rates, network users and threats.

Carrier cyber security platforms need to be able to cope with this increased network traffic rate and both intentional and unintentional impact of IoT devices. Multi-layered detection, quality threat intelligence, traversal of the physical and virtual domains, bringing together the network core and edge visibility and a granular forensics capability are all mandatory elements of these tools for effective network and security operations. These teams face challenges in bringing together the network signalling and device data behaviours in order to protect their customers, network infrastructure, services and brand.

References

[1] cybox. (2019). Cyber Observable eXpression (CybOX™) Archive Website. Available: https://cybox.mitre.org. Last accessed 1st April 2019.

[2] Mike Blunt. (2016). Why BGP Flowspec is a step forward in DDoS mitigation. Available: https://www.netcraftsmen.com/bgp-flowspec-step-forward-ddos-mitigation/. Last accessed 1st April 2019.

[3] Telesoft Technologies. (2019). Available: https://www.telesoft-technologies.com/. Last accessed 1st April 2019.

[4] Gartner. (2019). Available: https://www.gartner.com/en. Last accessed 1st April 2019.

[5] SAE Mobilus. (2018). Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Available: https://www.sae.org/standards/content/j3016_201806/. Last accessed 1st April 2019.

[6] Byron V. Acohido. (2019). The Dark Sides of Modern Cars: Hacking and Data Collection. Available: https://threatpost.com/modern-car-warning/142190/. Last accessed 1st April 2019.

[7] Vandana Sharma, Ravi Tiwari. (2016). A review paper on "IOT" & It"s Smart. International Journal of Science, Engineering and Technology Research (IJSETR). 5 (2), 472-476.

[8] Adi Roberston. (2018). California just became the first state with an Internet of Things cybersecurity law. Available: https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law. Last accessed 1st April 2019.

[9] Michael Cobb. (2015). What's the key to IoT device discovery in the enterprise?. Available: https://internetofthingsagenda.techtarget.com/answer/Whats-the-key-to-IoT-device-discovery-in-the-enterprise. Last accessed 1st April 2019.

[10] Shodan. (2019). Available: https://shodan.io. Last accessed 1st April 2019.

Headquarters
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
t. +44 (0)1258 480880
f. +44 (0)1258 486598
e. sales@telesoft-technologies.com

Americas
Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
e. salesusa@telesoft-technologies.com

Asia
Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301, India
t. +91 120 612 7725
e. salesindia@telesoft-technologies.com

telesoft-technologies.com