



Internet or Inter-Threat: Cybersecurity and the Next Generation of the Internet

Martin Bosshardt
CEO, Anapaya Systems AG

September 26, 2023

Internet – the largest network of networks



The growing internet...

- **4.8 zettabytes** annual global IP traffic
- **1.5 billion** websites
- **5.25 billion** users
- **15.14 billion** (IoT) connected devices



... is not adapted for the 21st century

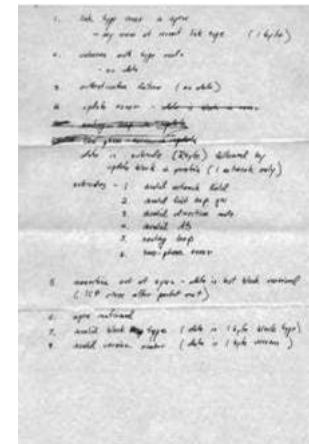
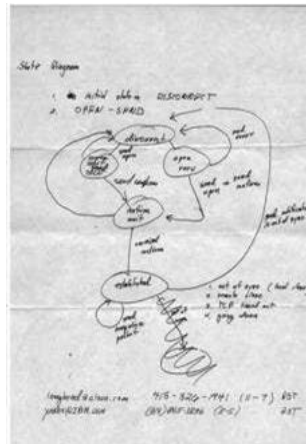
- Designed to **connect**, but not to **control**, leaving data is vulnerable to cyberattacks, including BGP hijacking and DDoS
- While you can adapt routing policies, users still have **no control** where their data is sent
- Data is often sent on the cheapest but slowest route, impacting service **reliability** and performance

The internet, as we know it, started with napkin scribbles over lunch



Kirk Lougheed of Cisco and Yakov Rekhter of IBM were having lunch in a meeting hall cafeteria when they wrote today's routing protocol on napkins.

A genius idea to introduce a compass system for data travelling across networks around the globe.



The Border Gateway Protocol (BGP*) was designed in 1989, when there were only **80 thousand** known hosts

There are over **1 billion** internet hosts today. The technology used - BGP, is unchanged

Internet – unlimited connections, unlimited exposure

The National Security Agency (NSA) and Federal Bureau of Investigations (FBI) have listed **16 flaws** in network device software from 10 brands, including:

citrix



FORTINET

MIKROTIK

NETGEAR

Pulse Secure

that were publicly disclosed between 2018 and 2021. Most of the flaws are rated as **critical**.

This is the **downside of unlimited reachability** for critical services.

Sources: [NSA & FBI Issue Warning for State-Sponsored Attacks that Exploit VPN Infrastructures; https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF](https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF)



NSA & FBI Issue Warning for
State-Sponsored Attacks
that Exploit VPN
Infrastructures



History of DDoS a concerning trend...



First deliberate DDoS attack
University of Illinois



1973

Spoofed SYN flood attacks emerge

1996

DNS amplification debuts



1999

2000

Windows-based DDoS botnets launched



1997

- DDoS extortion surfaces
- DNS query flood emerges

DDoS attacks surpass 10 Gbps

10 Gbps

2005

IoT botnet debuts

2008

2010

DDoS attacks surpass 100 Gbps

100 Gbps

2011

Lulzsec launches DDoS attack on government agencies
attacking CIA, US Senate, Public Broadcasting Service, and UK SOCA law-enforcement agency

DD4BC DDoS attack campaign
attacking cryptocurrency exchanges, online sports betting firms, financial institutions, ecommerce sites, and internet gambling firms

Operation Ababil launched
DDoS attack targeting US and EU financial institutions

2012

2014

DDoS attacks surpass 500 Gbps

500 Gbps

2015

DDoS attacks surpass 2.5 Tbps

2.5 Tbps

2017

Mirai source code released

2016

2019

Lazarus Bear Armada (LBA) DDoS extortion campaign attacks financial institutions



2020

DDoS attacks surpass 3 Tbps

>3 Tbps

2021

2022

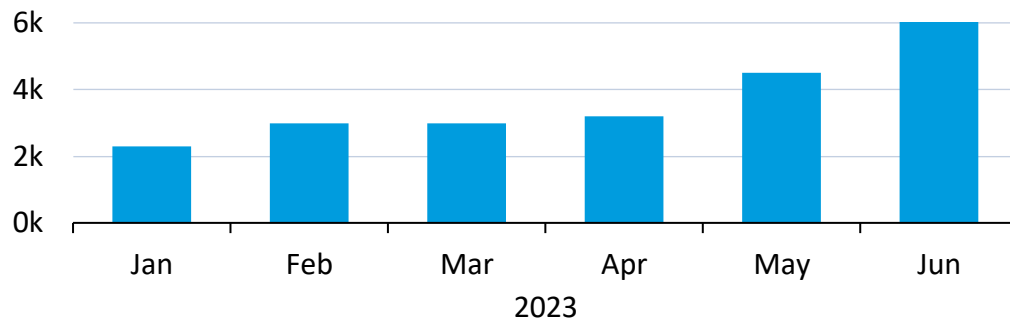
Killnet Group emerges
Pro-Russian hackers attack Ukraine supporters

DDoS attacks have been increasing in frequency



- > **115% increase** in DDoS Attacks worldwide from 2021 to 2022
- Cybercriminals increased their attention on **government, healthcare, and transportation systems** in 2Q23

DDoS attacks per month in Switzerland



Key Swiss institutions have been attacked



DDoS attacks on government administrations



DDoS attack on Ministries, Israel

Websites of the Israeli Health, Interior, Justice, and Welfare ministries were taken offline.



A kind of attack **characteristic of Russian patriotic hackers**

The largest-ever cyber attack carried out against Israel



This cyberattack is likely linked to the crisis in Ukraine.

Killnet DDoS attack against Prince of Wales

Pro-Russia hacker group Killnet launched the DDoS attack.



Attack on the **website belonging to the Prince of Wales**



The hackers warned the **UK healthcare system** would be next.

Killnet also threatened future attacks against the London Stock Exchange, the British Army, & more.

March 2022

March 2022

DDoS Attack Against the Ukrainian Ministry of Defense

A threat actor launched an HTTP-based DDoS attack against the webmail server belonging to the Ukrainian Ministry of Defense.



DDoS attack **using DanaBot**

Attempt to steal credentials using **download and execute commands**



The hacker used two stages of malware.

June 2022

DDoS attacks hit Norway

A DDoS attack temporarily knocked out public and private websites in Norway.

Suspension of online services for **several hours**



The attack came two days after a similar attack temporarily knocked out public and private websites in Lithuania.

The attack targeted a **secure national data network**

November 2022

June 2023

Attack on Swiss Federal Websites, Switzerland

The pro-Russian NoName hacker group claimed responsibility.

The attack also impacted the website functions of the Swiss National Railway system.



The attack was aimed at the **entire federal administration**

DDoS attacks on government administrations



March 2022

DDoS attack on Ministries, Israel

The websites of the Israeli Health, Interior, Justice, and Welfare ministries were taken offline.

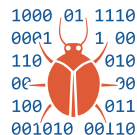
The cyberattack started at 6:15 PM and ended at 7:30 PM.

This cyberattack is likely linked to the crisis in Ukraine, given that Israel had begun to join other countries in placing sanctions against Russia.

A kind of attack
characteristic
of Russian
patriotic hackers



The
largest-ever
cyber attack
carried out against Israel



NEWS

DDoS barrage against Israel described as the "largest ever" cyberattack its faced



Cyber Israel

@Israel_Cyber · Follow

In the past few hours, a DDoS attack against a communications provider was identified. As a result, access to several websites, among them government websites, was denied for a short time. As of now, all of the websites have returned to normal activity.

@Israelgov

10:10 PM · Mar 14, 2022



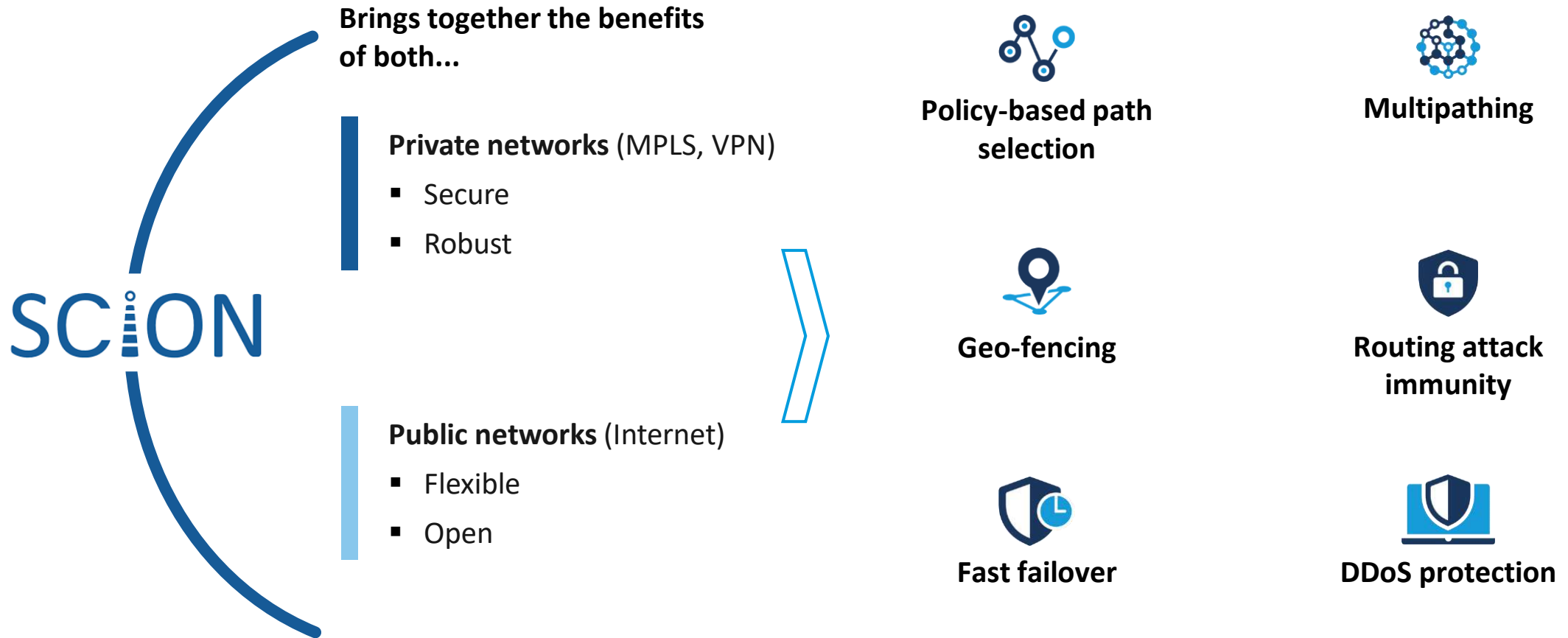


ANAPAYA

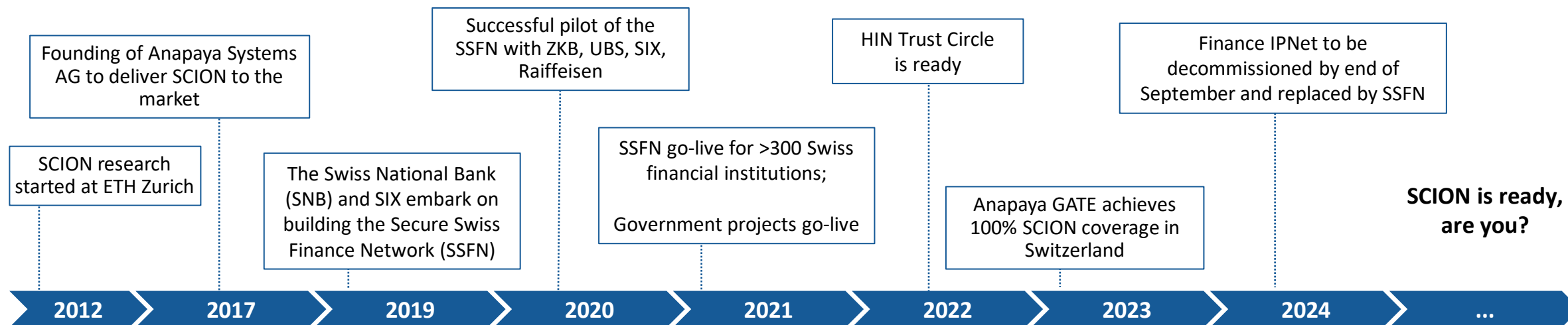


The solution

Anapaya is bringing the Internet to the next century



Over 10 years of research – SCION didn't happen over lunch



Our co-founder



"SCION is uniquely positioned as it solves the root causes of the Internet's security problems – in contrast to other solutions focused on solving symptoms."

Prof. Dr. Adrian Perrig of ETH Zurich
Department of Computer Science, Institute of Information Security, The Network Security Group

Partners



The SCION internet



The **future internet architecture** developed to enhance the **security, availability, and transparency** of data communication.

Simultaneous use of **several paths** allow for:

- Increased capacity
- Interruption-free failover
- Lower latency

Users can **choose paths** based on requirements

- Latency, drop rate, jitter
- Trust, geographical jurisdiction
- Cost
- CO₂ reduction



Legend

CORE
by ANAPAYA

EDGE
by ANAPAYA

GATE
by ANAPAYA

SSFN ecosystem



SNB and SIX launched the communication network SSFN (Secure Swiss Finance Network):
a dedicated multi-provider network for the **Swiss finance sector in the safest corner of the internet**

SNB and SIX launch the communication network Secure Swiss Finance Network

Helping to strengthen cyber resilience in the Swiss financial sector



Published at
15 Jul 2021

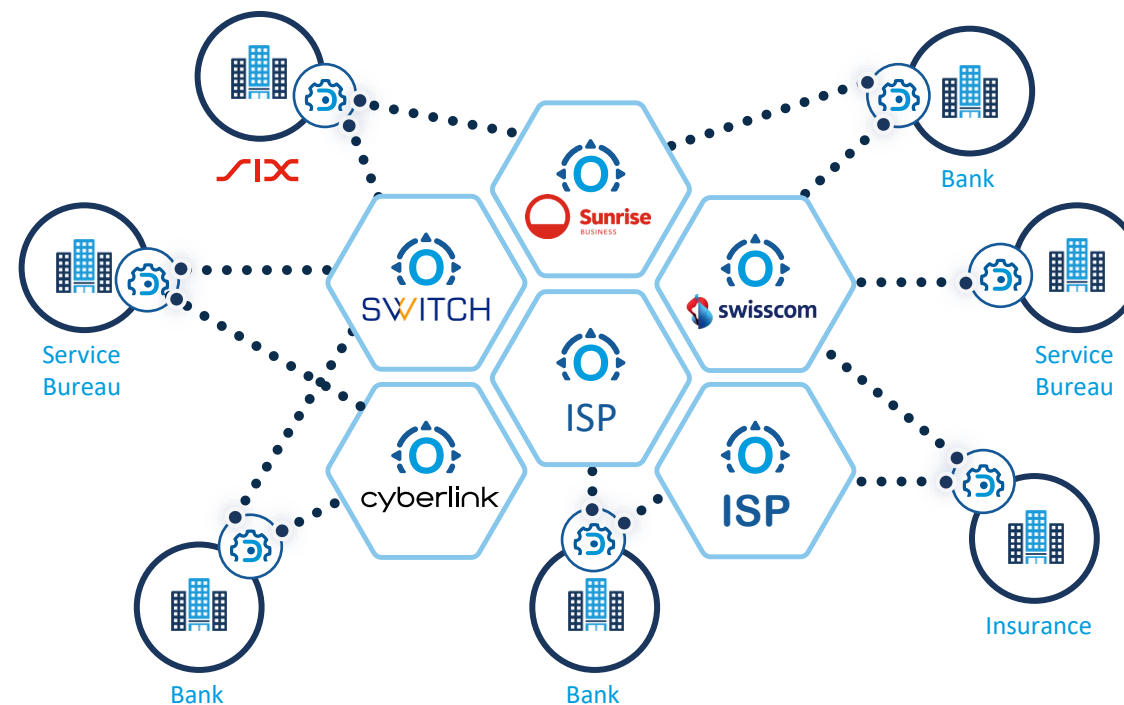
Medium
Media

Finance IPNet to Be Decommissioned in September 2024

At the end of September 2024, SIX will decommission Finance IPNet as the gateway to its infrastructure services. Secure Swiss Finance Network (SSFN) has proven successful as a communication service and will replace Finance IPNet as a gateway. Nothing will change for customers with other gateways to SIX (such as their own fiber optic cables).

Published at
20 Dec 2022

Medium
News



The **SSFN** has:


>300 participants, incl. banks, insurance companies, and securities firms

The **Swiss Interbank Clearing (SIC)** processes:

12.4 million payment transactions and
CHF 403 billion¹ turnover of on peak days

The SCION internet is proven to be more resilient



	 SSFN		Existing IP network	
Resilience test scenario	Failover time	Session upheld?	Failover time	Session upheld?
Link failure-access	< 1s	yes	> 3 min	no
Link failure-core	< 1s	yes	n/a	no
Core Router failure	< 1s	yes	n/a	no
EDGE Gateway failure	< 5s	yes	> 3 min	no
Provider failure	< 1s	yes	n/a	no



SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIONALE SVIZZERA
SWISS NATIONAL BANK



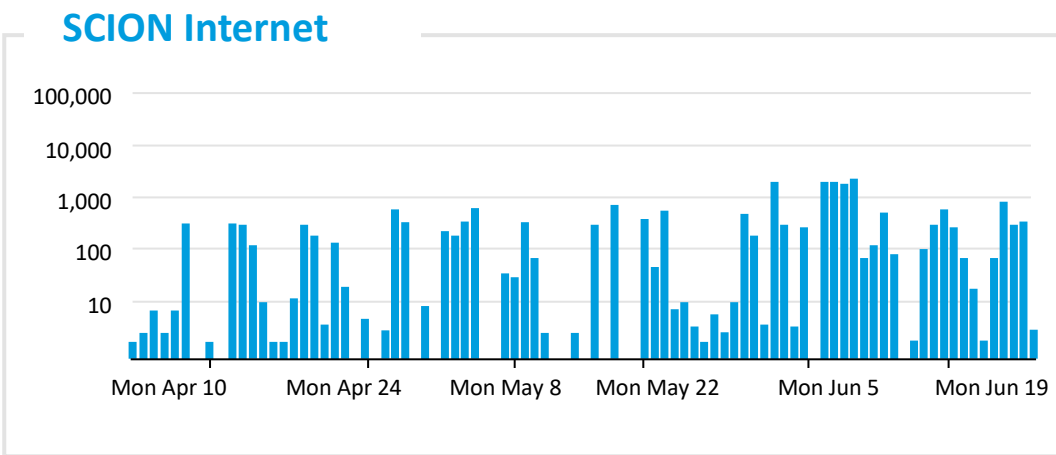
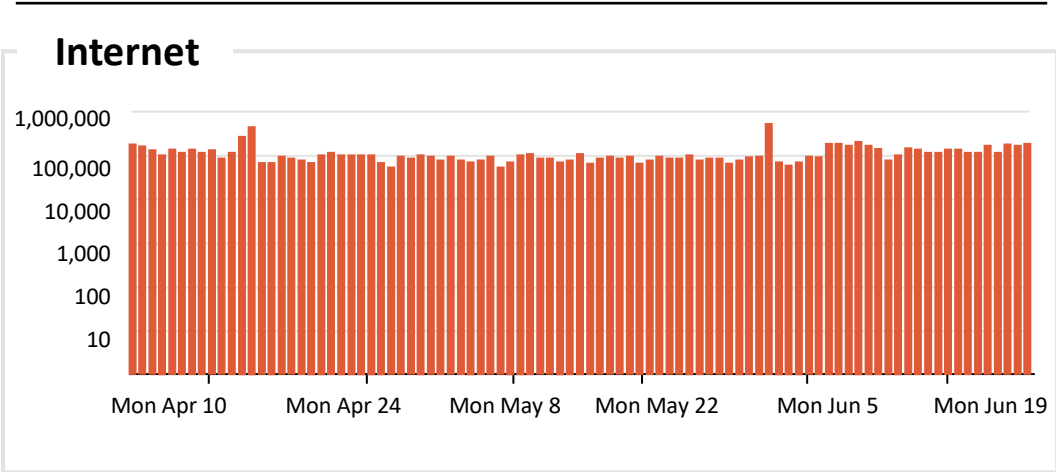
Fritz Steinmann, Senior Network Security Architect, SIX Group

“Extensive testing under extreme conditions has proven the reliability and resilience of the infrastructure—made possible by the path control and inherent multipathing properties of a SCION-based network architecture. This level of reliability and resilience is a vast improvement to ensure business continuity for current and future system-relevant use cases and applications not only in the financial sector but also for other critical infrastructures.”

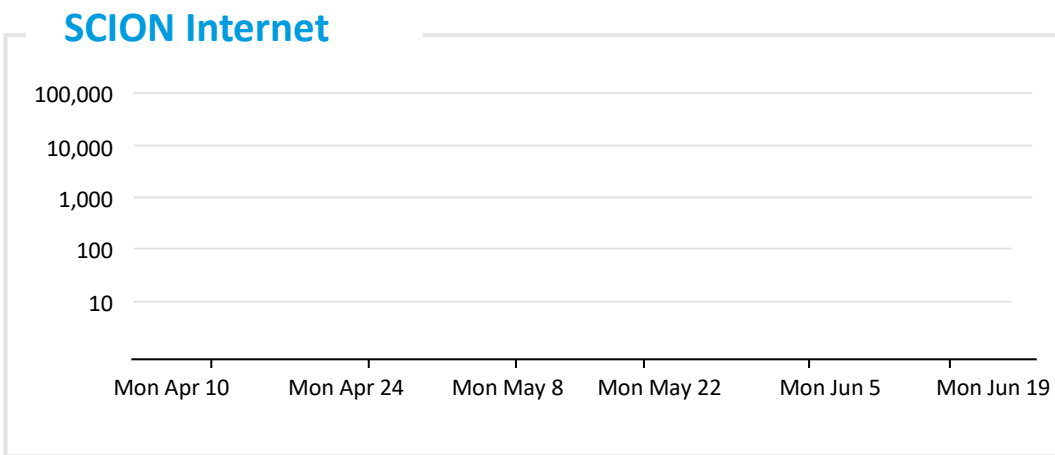
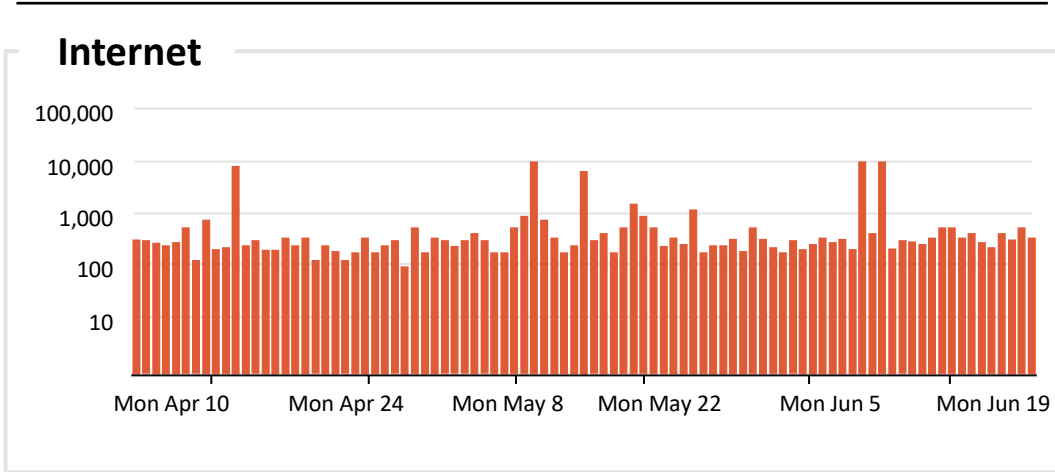
Proof Point: Prominent Swiss Bank in 2Q23



Attacks with unspecific intent



Attacks with malicious intent



The SCION internet has the trust of the Swiss industry



SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIONALE SVIZZERA
SWISS NATIONAL BANK



SSFN: Secure Swiss Finance Network

The new secure, reliable, community-based and sovereign network launched to interconnect **321 participants**, clearing **12.4 million payment transactions** and **CHF 403 billion¹ turnover** on peak days.



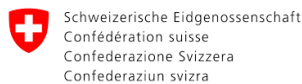
HIN Trust Circle

Improving the cyber-resilience of the health ecosystem in Switzerland by onboarding **~50k health professionals**.



Research and Education

ETH Zurich and SWITCH are leading the deployment of the SCION network for research and education in Switzerland and beyond, thanks to GÉANT.



Swiss Government and Energy

Several initiatives with the Confederation are now active at different levels: from the evaluation of the benefits for Cantons and Municipalities, to productive SCION connections between Asian locations and Switzerland. Discussions on connecting the energy sector are underway.



ANAPAYA

www.anapaya.net



Background

Martin Bosshardt

CEO, Anapaya Systems AG

Experience:

ABB

IEQT

 **eevolve**

 **opensystems**



westhive

**Y&R
GROUP
SWITZERLAND**

Education:

ETH zürich

Coollest personal accomplishment?

Building an atomic microscope

Superpower?

Building an exciting and fun corporate culture

