The Enduring Threat

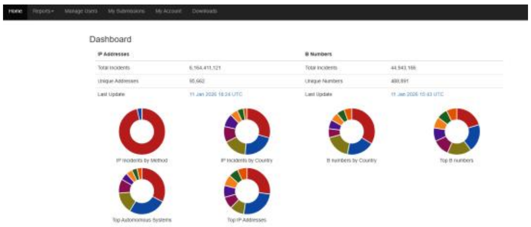
Real-time communications present continual interest to threat actors aiming to gain access to vital information, commit fraud, disrupt critical services, or commit other malicious activities. Potential attacks include: -

- Denial of Service attacks against device and cloud services
- Authentication attacks enabling unauthorised access to information
- Penetration attacks against devices and services
- Unauthorised monitoring or modification of data in transit

Continued vigilance is therefore necessary to determine sources and methods of attack and create and maintain methods of mitigation. Tools that enable accurate and effective data capture of live events on public networks are therefore crucial in threat recognition.

Attack Discovery

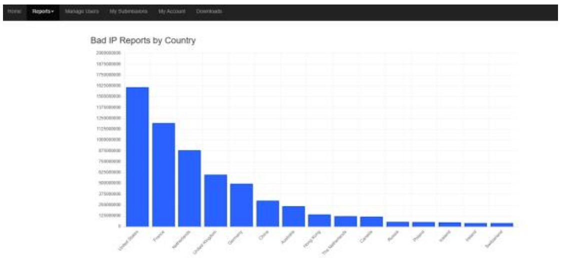
With many years of experience researching and developing effective security solutions for real-time communications applications, UM Labs operate an agile global honeypot network that collects, identifies, and analyses data on potential attacks.



Dashboard

IP Addresses		B Numbers	
Total Incidents	6,164,411,121	Total Incidents	44,943,166
Unique Addresses	95,662	Unique Numbers	488,891
Last Update	11 Jan 2026 16:34 UTC	Last Update	11 Jan 2026 15:43 UTC

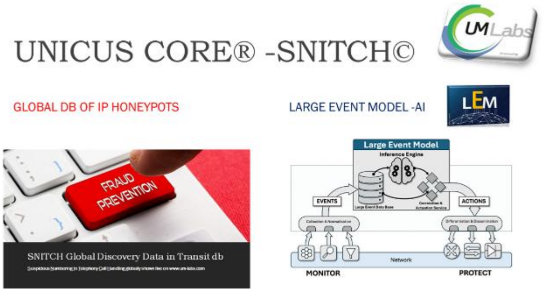
Known as SNITCH™ (Suspicious Numbering In Telephone Call Handling), the database system has collected data on a multiplicity of attacks focussed on call fraud for over more than a decade, constituting one of the world's most comprehensive repositories of threats to real-time communications applications.



SNITCH™ Access

The SNITCH™ repository is currently accessible via three separate interfaces; a GUI enabling investigators and research analysts to explore the repository in a granular manner, a data API that allows automated exploration and a provisioning data interface which enables data captured in the repository to be processed into provisioning actions to the Unicus® security technology – facilitating comprehensive response as part of a wider Large Event Model ("LEM") based automated multi-threat, multi-layer security solution.

SNITCH™ to UNICUS®


UNICUS CORE® -SNITCH©
GLOBAL DB OF IP HONEYPOTS
LARGE EVENT MODEL -AI
LEM
FRAUD PREVENTION
SNITCH Global Discovery Data in Transit db
Suspicious Numbering In Telephony Call Handling globally shown live on www.um-labs.com
Large Event Model
Inference Engine
Large Event Data Base
Correlation & Actuation Service
EVENTS
ACTIONS
Collection & Normalisation
Differentiation & Dissemination
Network
MONITOR
PROTECT

Providing over 6 billion IP protocol attacks from 100 countries and having verified data of 10 years, allows the prediction and proactive defence actions within the Unicus® Inference Core. All extended to include IP standards from IOT/EDGE.