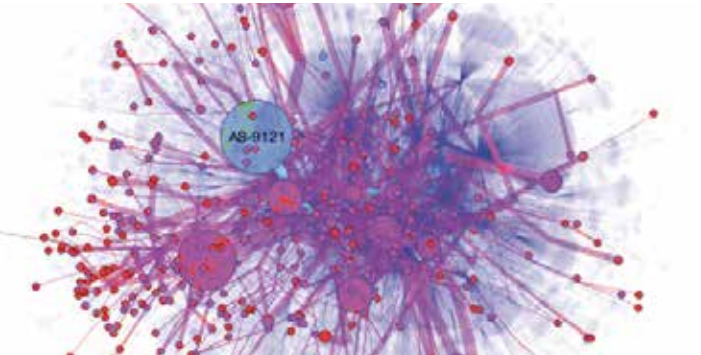
DETECTION OF ABNORMAL NETWORK BEHAVIOUR, ATTACK ATTRIBUTION AND BORDER GATEWAY PROTOCOL ANALYSIS

CONTACT

Internet Threat Landscape: A variety of data sets have been collected and analysed to explore the distribution of malware, the growth of botnets and the evolution of spam campaigns. The VIS-SENSE framework combines advanced data mining techniques with innovative visualizations to provide analysts with insights into the whole "Spam Lifecycle". New strategies for malware propagation could be identified along with instances of botnet cooperation in the form of "outsourcing".

Other Case Studies: The following less inclusive case studies have been conducted using the VIS-SENSE framework:

- Analysis of data collected by intrusion detection systems to automatically find and characterise common intrusion patterns and use these to provide situation awareness.
- Analysis of login procedures to characterise suspicious or unauthorised access to user accounts.
- Analysis of SSL certificate hierarchies derived from a scan of the Internet for the detection of anomalies.



COORDINATOR:

Dr. Jörn Kohlhammer
Fraunhofer IGD
Fraunhoferstrasse 5
64283 Darmstadt
Germany

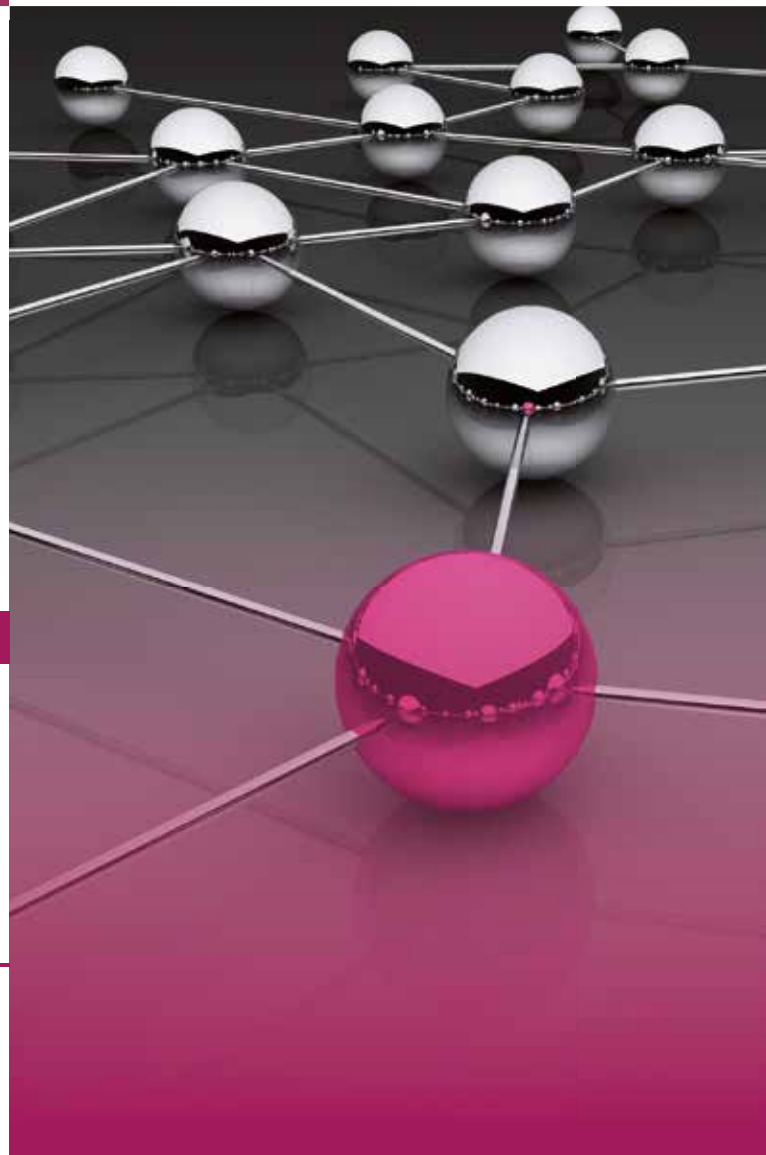
E-mail: joern.kohlhammer@igd.fraunhofer.de
Phone: +49 6151 155-646
Fax: +49 6151 155-139
Website: www.vis-sense.eu

PARTNERS:

Universität Konstanz
Symantec
EURECOM
TELECOM SudParis
CENTRE FOR RESEARCH AND TECHNOLOGY - HELLAS INFORMATICS & TELEMATICS INSTITUTE
Fraunhofer IGD
SEVENTH FRAMEWORK PROGRAMME

VIS-SENSE

VISUAL ANALYTICS FOR ENHANCED NETWORK SECURITY

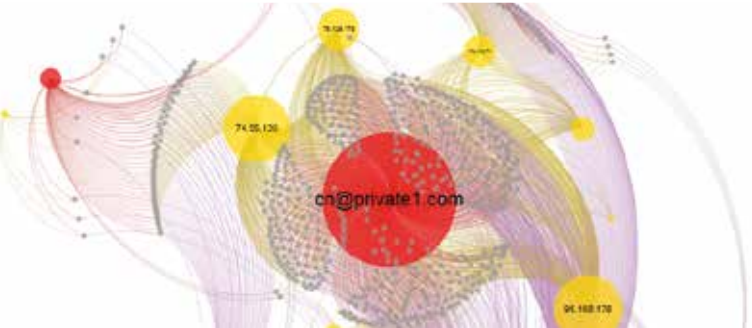


EXTENSIBLE, SCALABLE VISUAL ANALYTICS

The VIS-SENSE framework is a suite of visualization and data-mining technologies which aims to provide visual analytics for enhanced cyber security. By combining the strengths of people and computers the identification of suspicious actions in large networks can be improved.

The VIS-SENSE framework has been applied to application areas ranging from network information security and attack attribution to attack prediction and the detection of BGP hijacking. It addresses both the tactical (monitoring in real time) and strategic (long term) aspects of security.

The VIS-SENSE framework is the result of an EU-funded, focused research project involving six experienced partners from research and industry. The framework was conceived and built by some of the leading researchers in the fields of visual analytics and network security. It incorporates the next generation of tools to enable the interactive mining and visualization of large security-relevant data sets.



TARGET GROUPS

Telecommunications operators and ISPs: The VIS-SENSE framework addresses BGP hijacking and attack attribution. The rapid identification of malicious traffic is important for the protection of customer networks. The ability to warn customers about possible BGP hijackings would enable them to react quickly.

Security software companies: The VIS-SENSE framework enables threat and malware analysts to identify criminal campaigns in massive amounts alerts. The strategic analysis of the threat landscape improves their understanding of the modus operandi of attackers and its evolution over time.

Computer Emergency Response Teams (CERTs):
Both the tactical and strategic analysis of security data sets play a role in CERT work. The VIS-SENSE framework helps them to respond more effectively to security incidents but also to remain informed of changes in the attack phenomena they are monitoring.

Security researchers:
Besides using and testing the VIS-SENSE framework with their own data sets, researchers will be interested in improving and extending the framework with new visualizations and data-mining modules.

CASE STUDIES

BGP: Raw routing information has been collected from a series of BGP vantage points and analysed. The VIS-SENSE framework enables the detection and investigation of routing anomalies and of possible BGP hijacks. A variety of measures are correlated to reduce the number of false positives. The forwarding paths at the IP and AS levels towards specific suspicious IP addresses or networks have been monitored. When enriched with BGP routing information, routing anomalies and possible BGP hijacks could be monitored in both the data plane (IP) and the control plane (BGP).