Selex ES
A Finmeccanica Company

Cyber Security & Information Assurance

CNI, INDUSTRIAL & SCADA CYBER PROTECTION

The Dragonfly hacking team has targeted thousands of systems within energy companies of the United States and Europe, successfully stealing valuable information in what appears to be a further step in the cyber battle following the Stuxnet attack in 2010.

Malicious malware software (HAVEX & Karagany) was used to compromise a number of computers running Industrial Control Systems (ICS). Data was subsequently harvested from the infected machines utilizing payloads designed for a specific industrial protocol. The attackers reached the victims through e-mail, hacking ICS vendors and other websites legitimately used by people from the energy sector.

Security analysts have identified and analysed several variants of HAVEX, which contacted C&C servers to transfer the stolen information. In addition to the theft of local information, many of the variants tried to interrogate the network in the search for OPC protocol servers.

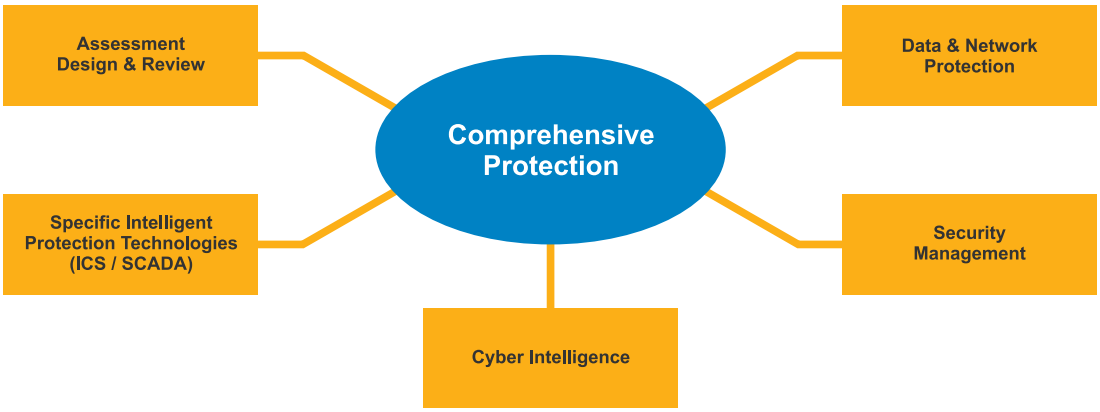
Through the components of its “Comprehensive Protection” programme, focused on Industrial & CNI Cyber Security, Selex ES offered its customers off-the-shelf protection from the Dragonfly threat and offers out-of-the-box protection from similar unknown threats. The solution relies on behavioural analysis to recognize the threat and promptly activate remediation actions.

The protection algorithms learn the “normal” behaviour of the industrial network and signal anomalies and deviances from the normal state. In particular for HAVEX & Karagany, the monitoring technologies recognise system behavioural anomalies at different levels.

This can include:

- Unusual network scanning
- Unusual use of specific Operating Systems features, such as accessing rarely used communication interfaces

Suspect activity will subsequently activate an alarm in the system, triggering timely remediation as appropriate.



COMPREHENSIVE CYBER PROTECTION FOR CNI

Selex ES Comprehensive Protection for Industrial & CNI Cyber Security combines a long experience in the Military and CNI fields, advanced proprietary developments and state-of-the-art technologies supplied by selected partners.

Comprehensive Protection is a modular offering divided into five areas:

Consultancy, assessment, design and review

- Audit and Advisory consultancy
- Organisational and Governance design
- Technical design and delivery
- Compliance
- Training

Data & Network Security

- Identity Management
- Network Security & Perimeter Defense
- Advanced Persistent Threat Protection
- Policy and Compliance
- Network Segregation
- Data Protection
- Forensics

SCADA/ICS specific protection technologies

- Automated asset discovery and vulnerability management
- Asset management
- Policy Audits
- Vulnerability control
- Self-learning network monitoring

Security Management

- Centralised management
- Response coordination
- Threat and incident analysis
- Continuity and recovery plans
- Service resilience

Intelligence

- Security Trends
- Predictive & Sentiment Analysis
- Early Warning, Anti Phishing
- OSINT & Advanced Detection
- Monitoring & Event Correlation
- Reporting

Compliances

LOCATIONS

Selex ES Spa
Piazza Monte Grappa 4
00195 Rome

Selex ES Ltd
430 Bristol Business Park
Coldharbour Lane
Bristol BS16 1EJ

Email: infomarketing@selex-es.com

OTHER PRINCIPAL OFFICES

Basildon, Essex, Chieti, Edinburgh, Luton, Milan, Rome, Southampton, Genoa

OTHER COUNTRIES

Brazil, India, Kingdom of Saudi Arabia, Romania, Turkey, United States

For more information please email **infomarketing@selex-es.com**
Selex ES S.p.A. - A Finmeccanica Company
Via Laurentina, 760 - 00143 Rome - Italy - Tel: +39 06 50271 - Fax: +39 06 5051140