Monitoring applications to increase security in 40G and 100G networks

Cyber Security and Today’s Communication Technologies

TPEB workshop, 30.1.2014

INVEATECH

Petr Kastovsky
kastovsky@invea.com

Company Introduction

INVEATECH

- Czech university spin-off company
- Established in 2007
- 26 employees, $ 3M revenue
- Key focus
  - **Hardware acceleration and FPGA Solutions**
  - **Flow Monitoring and Network Behavior Analysis**
  - **Lawful Interception and Data Retention**
- Products deployed at 500+ customers worldwide

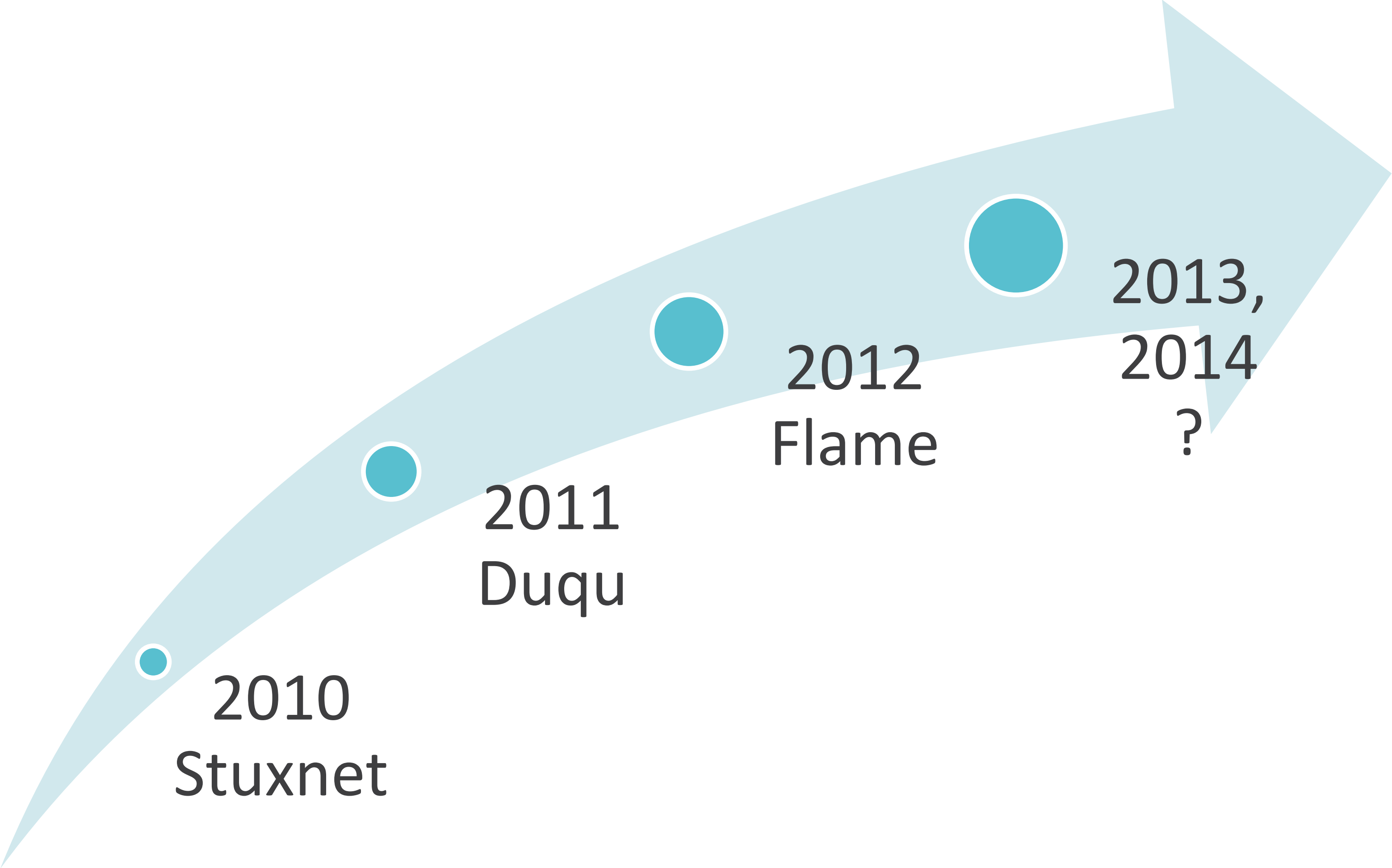
vmware PARTNER TECHNOLOGY ALLIANCE

CISCO DEVELOPER Registered

Gartner Research ID Number: G00208386

CERTIFICATE OF ACHIEVEMENT Deloitte.

Modern threats



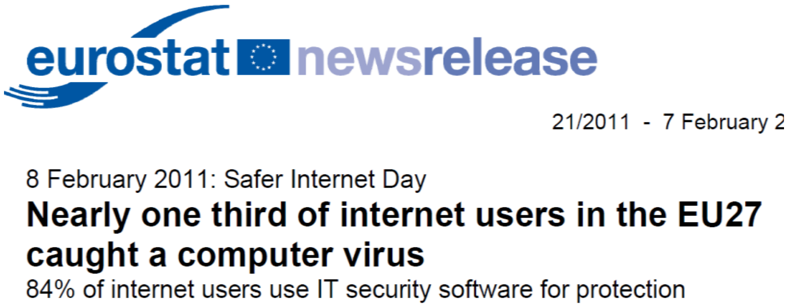
2010
Stuxnet

2011
Duqu

2012
Flame

2013,
2014
?

Modern threats

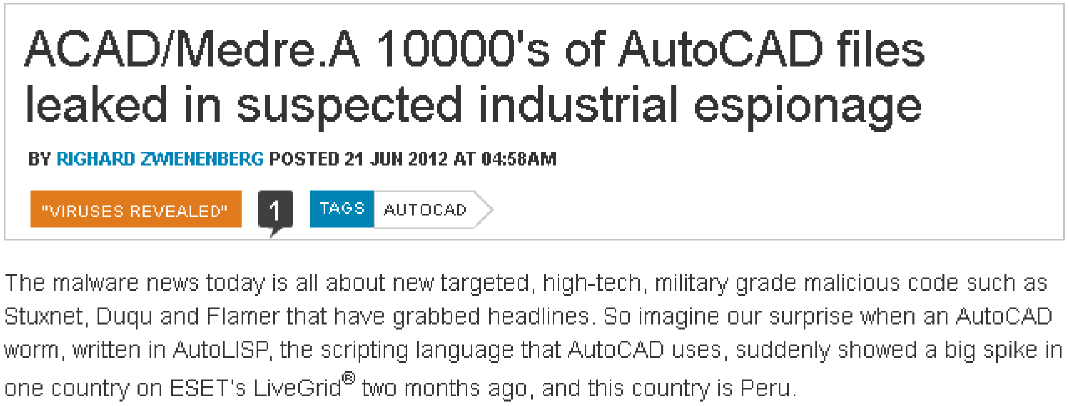


21/2011 - 7 February 2

8 February 2011: Safer Internet Day

Nearly one third of internet users in the EU27 caught a computer virus

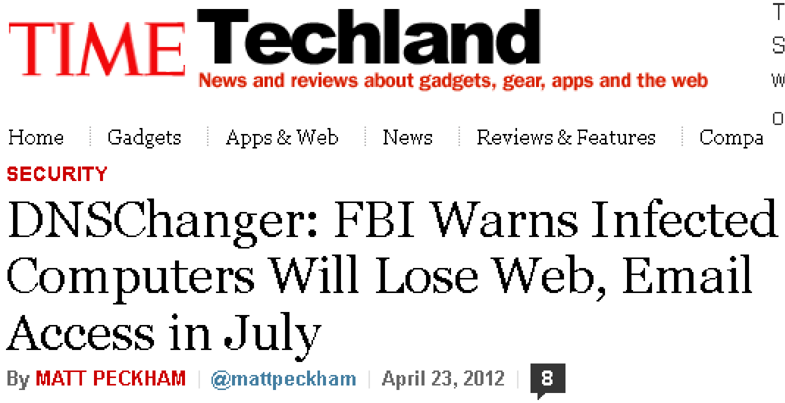
84% of internet users use IT security software for protection



ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage

BY RICHARD ZWIENENBERG POSTED 21 JUN 2012 AT 04:58AM

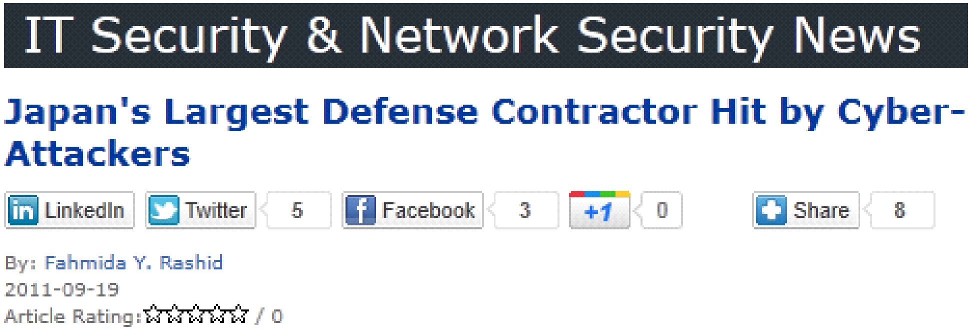
The malware news today is all about new targeted, high-tech, military grade malicious code such as Stuxnet, Duqu and Flamer that have grabbed headlines. So imagine our surprise when an AutoCAD worm, written in AutoLISP, the scripting language that AutoCAD uses, suddenly showed a big spike in one country on ESET's LiveGrid® two months ago, and this country is Peru.



SECURITY

DNSChanger: FBI Warns Infected Computers Will Lose Web, Email Access in July

By MATT PECKHAM | @mattpeckham | April 23, 2012 | 8

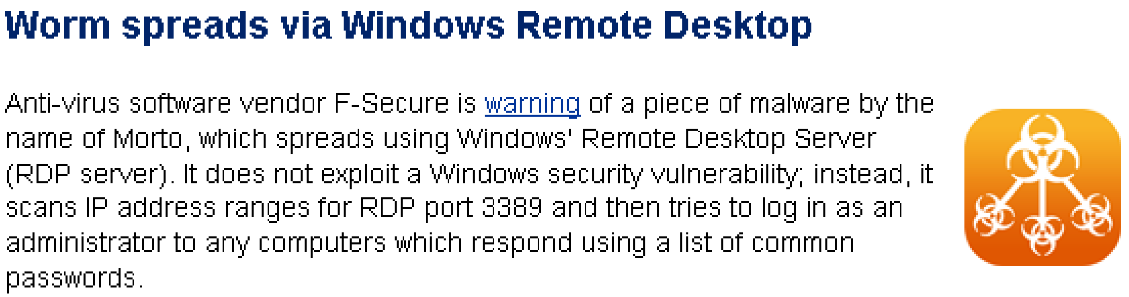


IT Security & Network Security News

Japan's Largest Defense Contractor Hit by Cyber-Attackers

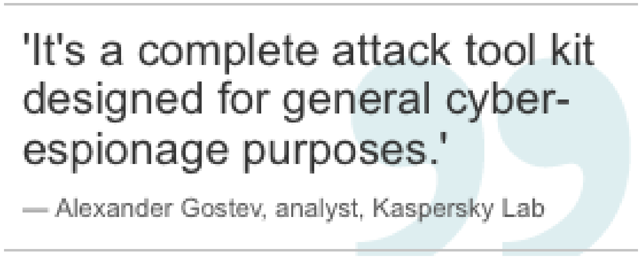
By: Fahmida Y. Rashid
2011-09-19
Article Rating:☆☆☆☆☆ / 0

29 August 2011, 13:27



Worm spreads via Windows Remote Desktop

Anti-virus software vendor F-Secure is warning of a piece of malware by the name of Morto, which spreads using Windows' Remote Desktop Server (RDP server). It does not exploit a Windows security vulnerability; instead, it scans IP address ranges for RDP port 3389 and then tries to log in as an administrator to any computers which respond using a list of common passwords.



> 'It's a complete attack tool kit designed for general cyber-espionage purposes.'
>
> — Alexander Gostev, analyst, Kaspersky Lab

Modern threats

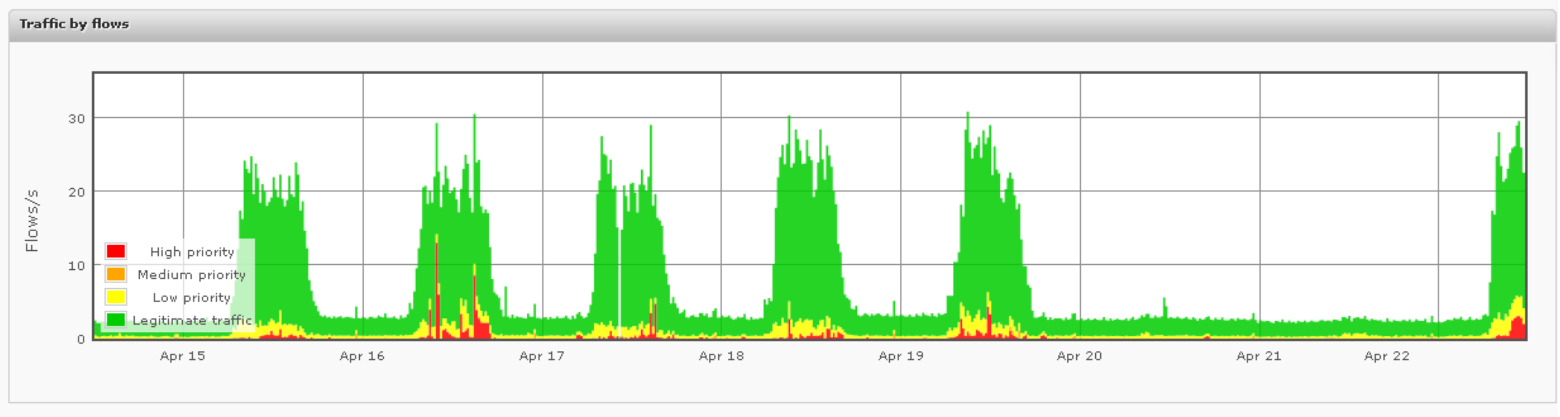
- Advanced Persistent Threats (APTs)
- Industry espionage and targeted attacks
- Zero-day attacks and polymorfic malware

- Application awareness
  - HTTP is a new IP
  - Application specific attacks
  - More and more services delivered on-demand

Security solutions

- Automatic, deep inspection
- Need to be smart, fast and flexible

- Visibility is the key



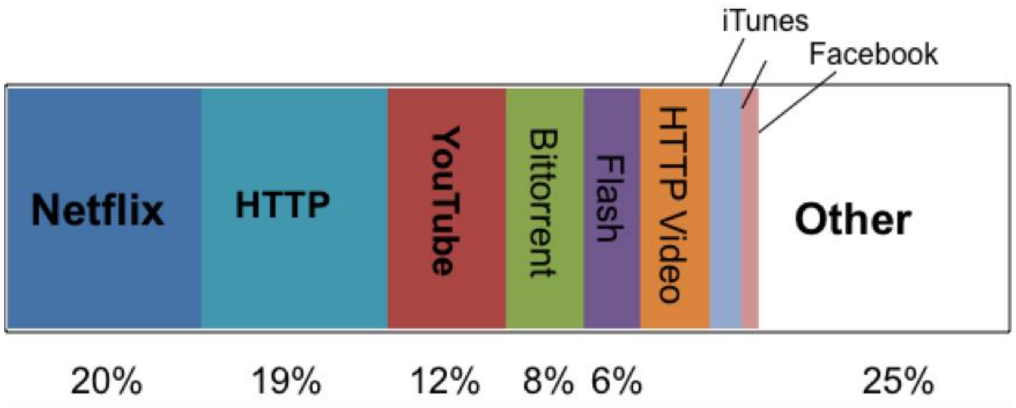
Challenges

- Typical deployment in core network
  - **high bandwidth** and line utilization
- New **link layer technologies** (10G, 40G, 100G)
- Growing **number of end users and devices**
- Growing **number of services**

- A lot of different network protocols
- Predicted growth of network traffic variability
- Limited computational resources

Next generation monitoring

- Dynamic level of detail, heavy tail distribution



- Novel approach of software defined monitoring
  - Analogy to software defined networking
  - Abstraction of monitoring functions
  - Flexible application protocol analysis

Software defined monitoring

- *Hardware* provides various methods of packet preprocessing
  - *The Muscles*

- *Software* controls the usage of preprocessing on flow basis
  - *The Controller*

- *User applications* request the HW acceleration and perform advanced monitoring tasks
  - *The Intelligence*

Applications can adjust acceleration of traffic processing according to their actual needs

Hardware Part

- Driven by instructions from „intelligent“ software
  - Hardware as fast as possible
- Well-defined set of operations:
  - Forward (cut) packet to a receive queue
  - Send unified headers to a receive queue
  - Update flow cache entry
    - create, remove, reset, export
  - Drop packet
- Configurable, flow aware distribution of traffic into receive queues

Software Part

- *Monitoring applications* in SW
  - process traffic from receive queues
  - determine the traffic of interest
  - instruct SW controller
- *SW controller* configures HW so that monitoring applications
  - *always* get what they asked for
  - get *the least* undesired traffic
- Application parsers for selected protocols
  - VoIP, DNS, SMTP etc.

Use Cases

- NetFlow statistics
- Application protocol parsing
- Application specific statistics
- Lawfull interception
- Forensic analysis of network traffic
  - zoom-in on suspicious data
- Active network device
  - accelerated switch, router, next-gen firewall, UTM …
- Acceleration of turnkey applications

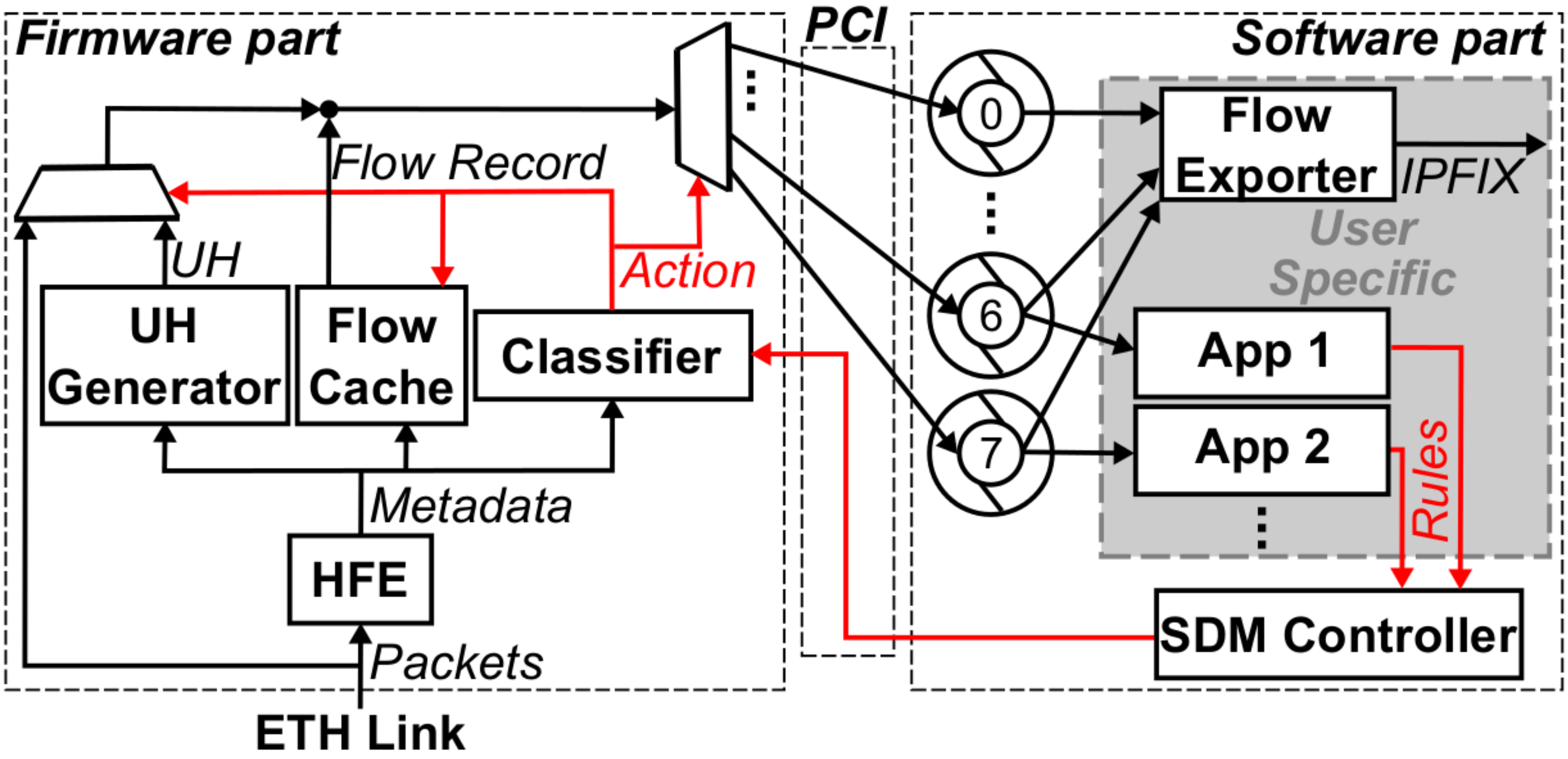
Platforms

- **Dedicated hardware**
  - High I/O performance
  - Expensive, limited flexibility

- **Commodity hardware**
  - Cheap and flexible
  - Limited I/O performance

- **Commodity hardware + Hardware acceleration**
  - **Multi-core CPUs + FPGA network interface card**
  - **High I/O performance**
  - **Reasonable price**
  - **Flexible**

Architecture



Summary

- Fully software controlled hardware accelerator
- Flow based measurements at speeds over 100 Gbps
- Easy deployment of new tasks without HW modifications
  - but supports specific HW measurements when needed
- Helps to accelerate application level processing
- Many opportunities for academic cooperation

Reference

upc
AVG
T··Mobile·
Belnet
dedicated connectivity
SLOANE PARK
Government of the Czech Republic
Ostrava Airport
T··Com·
UNIQA
Allianz
KONICA MINOLTA
CZECH STATISTICAL OFFICE
THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC
NK
IBP
Institute of Biophysics
VEOLIA
AEGON
e·on IT
SIEMENS
TELECOM Bretagne
eustream
pitcom
dm
MVV Energie
Matador
PX
PRAGUE STOCK EXCHANGE
BURZA CENNÝCH PAPÍRŮ PRAHA
ihp
zenit elektro
OUTSOURCING SOLUTION
ATComputers
kt
AVE
CSIRT-MU
Marius Pedersen
TE
THOMAYEROVA NEMOCNICE PRAHA 4
FAKULTNÍ NEMOCNICE OLOMOUC
UNIVERSITAS MASARYKIANA BRUNENSIS
ČD-Telematika
CASABLANCA INT
GEANT2
CARNet
BRNO UNIVERSITY OF TECHNOLOGY
Tomas Bata University
grnet
SURF NET
SWITCH
TÜBİTAK
ULAKBİM
UNIVERSITY OF TWENTE.
Olomoucký kraj
Kraj Vysočina
OLOMOUC

INVEATECH

High-Speed Networking Technology Partner

Petr Kastovsky
kastovsky@invea.com
+420 774 799 726

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno, Czech Republic
www.invea.com