FPGA accelerated application monitoring in 40 and 100G networks

Campus network monitoring and security workshop

CESNET workshop, 24.4.2014

Petr Kastovsky
kastovsky@invea.com

Company Introduction

INVEATECH

- Czech university spin-off company
- Established in 2007
- 40+ 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

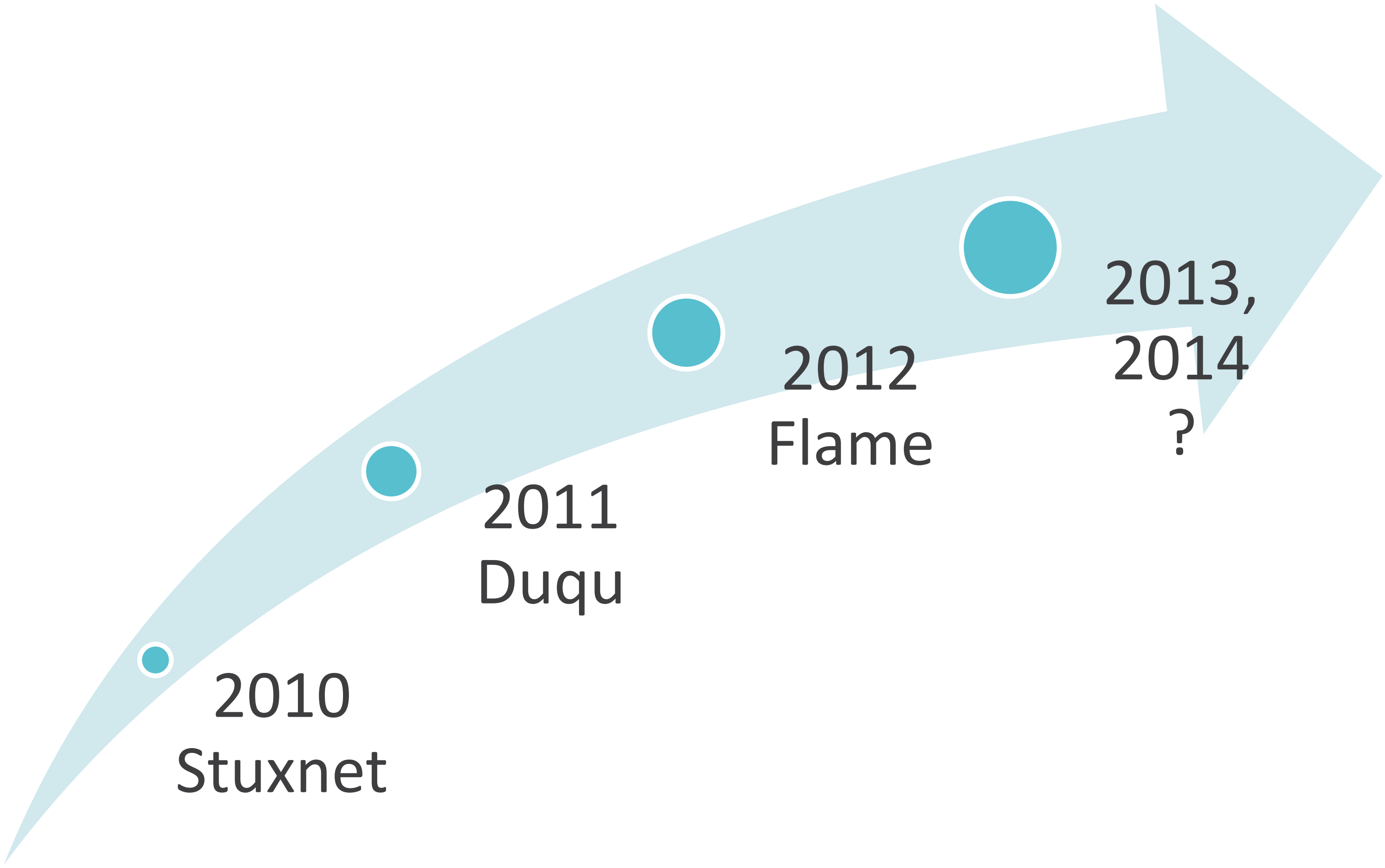
CISCO DEVELOPER Registered

Gartner Research

ID Number: G00208386

CERTIFICATE OF Deloitte. ACHIEVEMENT

Modern threats



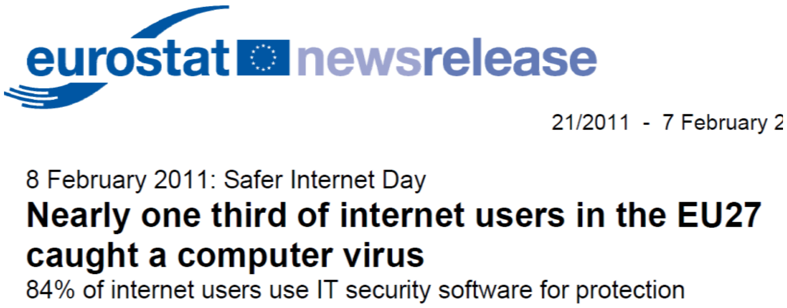
2010
Stuxnet

2011
Duqu

2012
Flame

2013,
2014
?

Modern threats



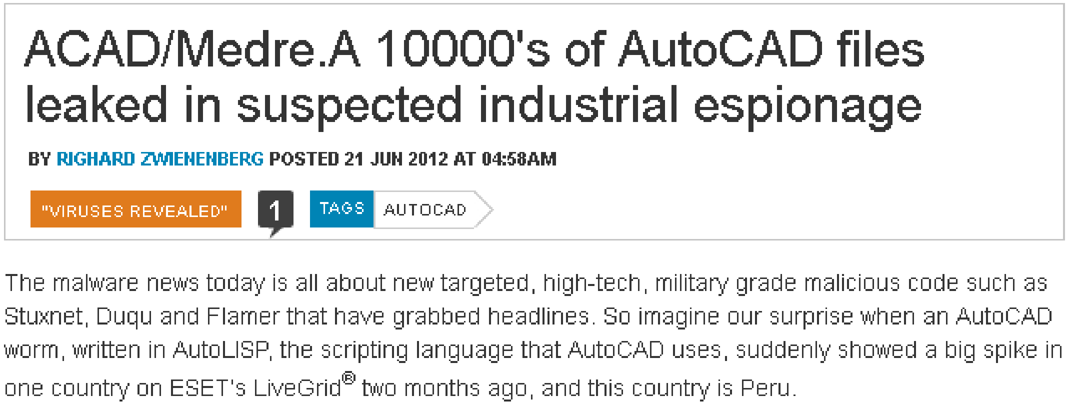
eurostat newsrelease

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

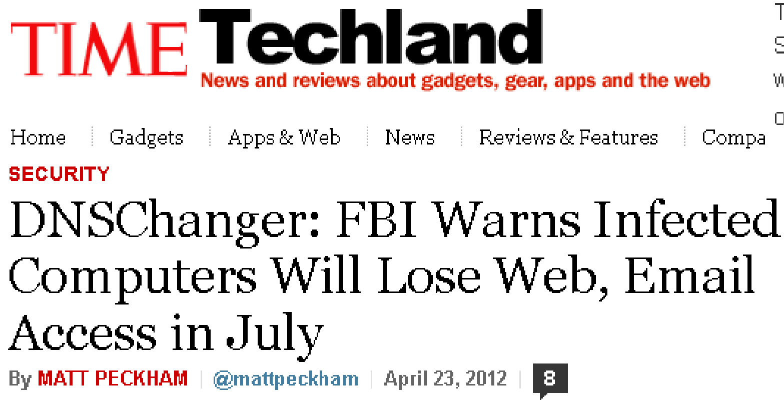


ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage

BY RIGHARD ZWIEHENBERG POSTED 21 JUN 2012 AT 04:58AM

"VIRUSES REVEALED" 1 TAGS AUTOCAD

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.



TIME Techland

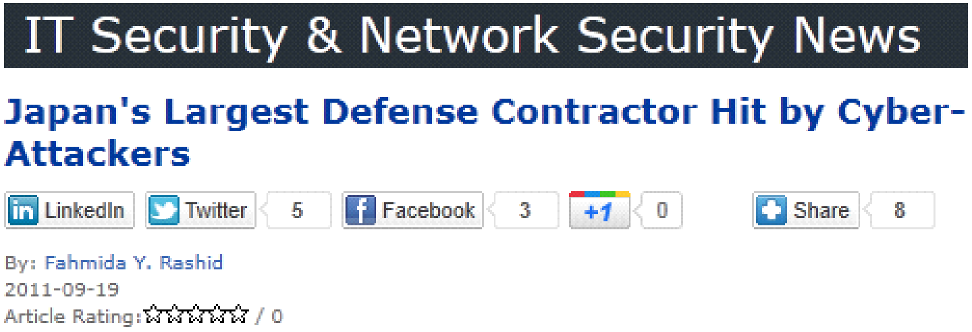
News and reviews about gadgets, gear, apps and the web

Home | Gadgets | Apps & Web | News | Reviews & Features | Compa

SECURITY

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

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



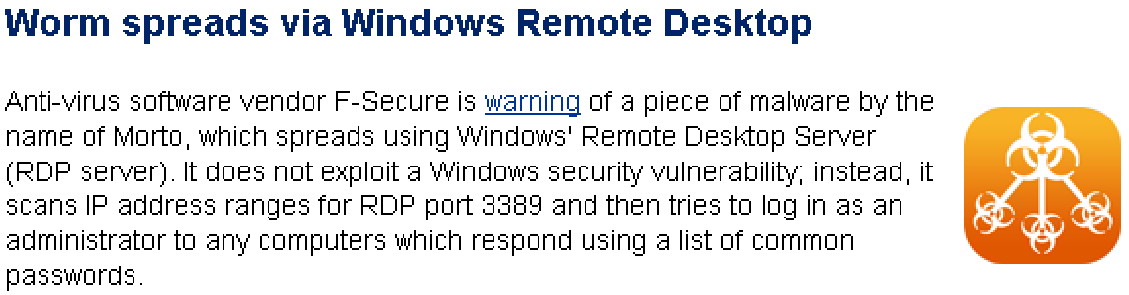
IT Security & Network Security News

Japan's Largest Defense Contractor Hit by Cyber-Attackers

LinkedIn | Twitter 5 | Facebook 3 | +1 0 | Share 8

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 polymorphic malware
- Application specific attacks (Bleeding heart etc.)

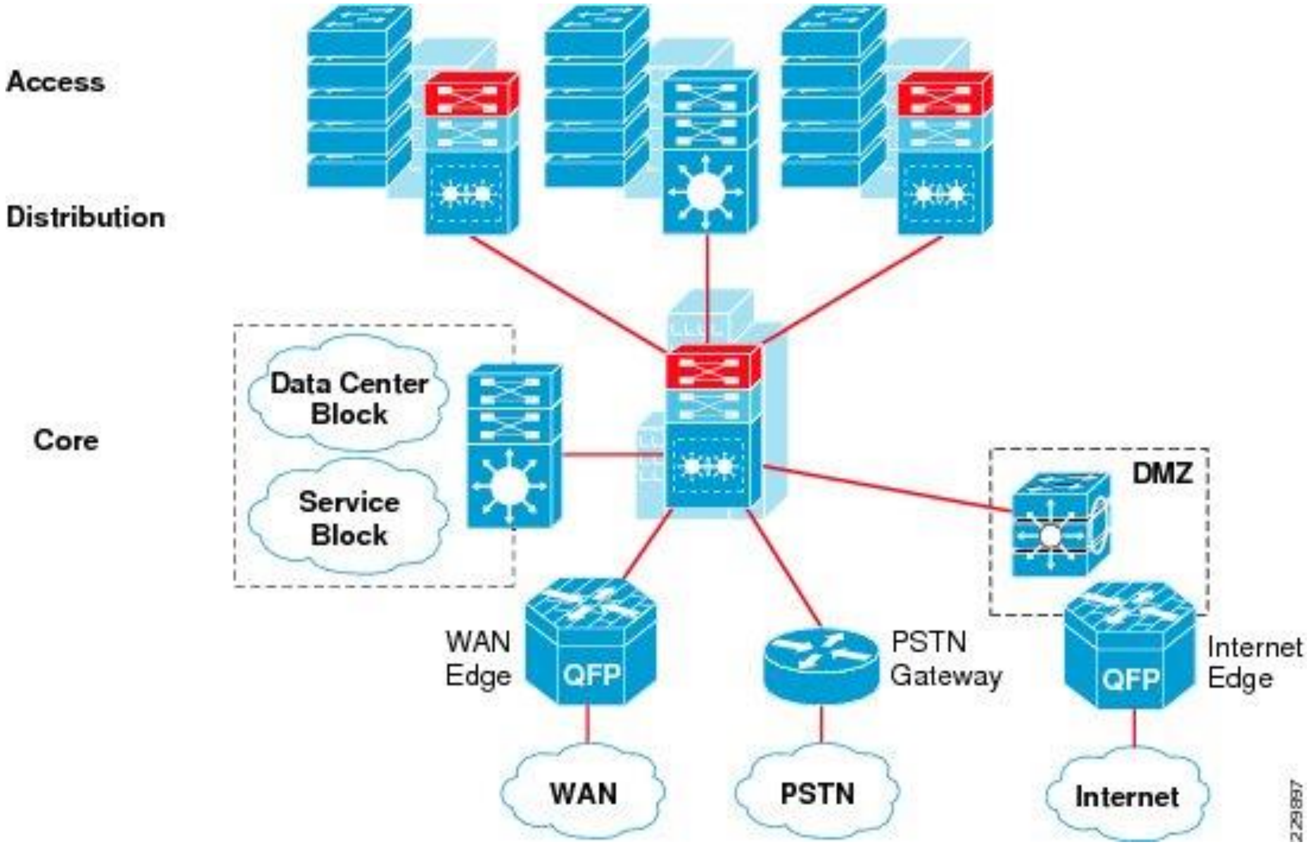
Security tools

- Wireshark
  - *www.wireshark.org*
- Snort
  - *www.snort.org*

- tcpdump
  - *www.tcpdump.org*
- FlowMon
  - *www.invea.com/en/go/flowmon*

- It all goes down to packet processing and analysis

Campus environment



Source: CISCO: Borderless Campus Design and Deployment Models

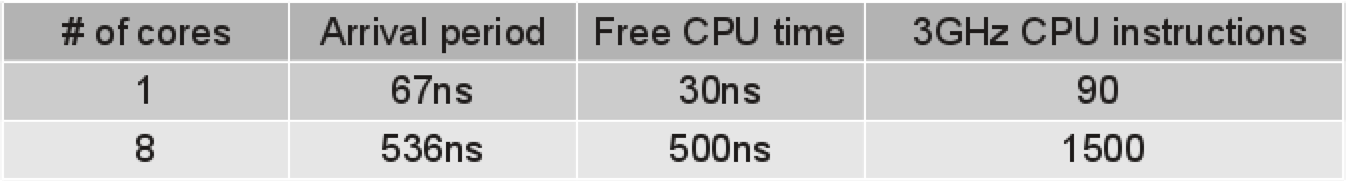
Campus environment

- Access layer – 1G
- Core, distribution layer – 10G

- Challenges
  - **High bandwidth** and line utilization
  - **Transition to 40G, 100G technologies**
  - Growing **number of end users and devices**
  - Growing **number of services**

Workload

- **1G Ethernet**
  - Max load 1,48 Mpps, new packet every 670ns
  - Standard network interface cards
  - Single CPU core provides enough horse power
- **10G Ethernet**
  - Max load 14,88 Mpps, new packet every 67ns
  - Network cards optimized for monitoring
  - Multiple CPU cores horse power
  - Smart traffic distribution necessary



# of cores	Arrival period	Free CPU time	3GHz CPU instructions
1	67ns	30ns	90
8	536ns	500ns	1500

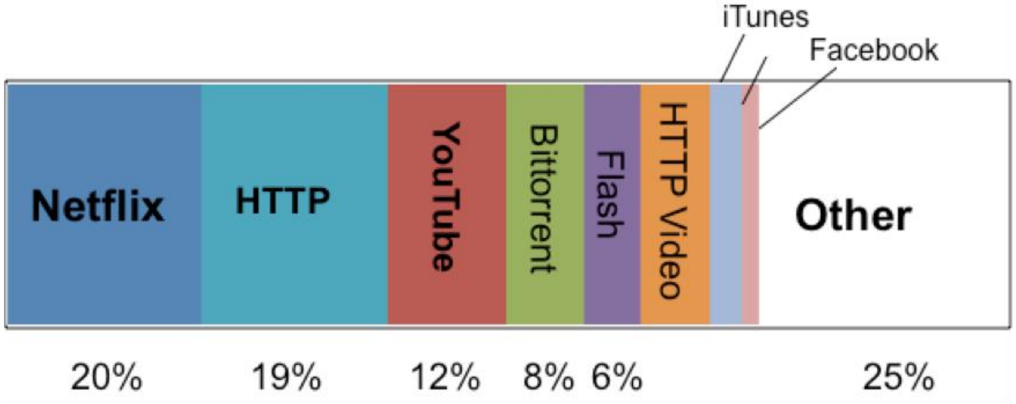
Workload

- **40G Ethernet**
  - Max load 59,5 Mpps, new packet in every 16,8ns
  - 5GB/s (DVD), 300GB/min, 18TB/h, 432TB/day
  - ~ 100 000 DVDs a day

- **100G Ethernet**
  - Max load 148,8 Mpps, new packet in every 6,7ns
  - 12,5GB/s (~3 DVDs), 750GB/min, 45TB/h, 1080TB/day
  - ~ 250 000 DVDs a day → 300m tall column
  - Smart traffic filtering necessary

Smart filtering

- What can be dropped?



- When it can be dropped?
  - Only when it is known what is being dropped!

Smart filtering

- **What do we need?**
  - Fast and efficient packet filtering – *to drop*
  - Intelligent and flexible traffic decoding – *when we know what*

Platforms

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

Smart filtering

- What do we need?
  - Fast and efficient packet filtering – *to drop*
  - Intelligent and flexible traffic decoding – *when we know what*

- Problems
  - ***Too many packets for software processing***

Platforms

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

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

Smart filtering

- What do we need?
  - Fast and efficient packet filtering – *to drop*
  - Intelligent and flexible traffic decoding – *when we know what*

- Problems
  - Too many packets for software processing
  - ***Traffic decoding too complex for hardware***

Platforms

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

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

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

Smart filtering

- What we need?
  - Fast and efficient packet filtering – *to drop*
  - Intelligent and flexible traffic decoding – *when we know what*

- Problems
  - Too many packets for software processing
  - Traffic decoding too complex for hardware

- **Hardware-software co-design**
  - **Filtering in hardware, decoding in software**

HANIC

- Next generation of packet capture
- **FPGA card**
  - 80G – 2x 40G, 8x 10G, PCI-E gen3 x8
  - 100G – 1x 100G (CFP2), PCI-E gen3 x16

- **Firmware**
  - Well-defined set of fast operations
  - Forward, cut, drop, extract UH, update flow entry
- **Software**
  - Drivers, tools, libraries, API
  - Application decoders (DNS, HTTP, VoIP …)

Summary

- Fully software controlled hardware accelerator
  - Joint development effort with CESNET and UNIs
- Abstraction of network monitoring functions
  - Inspired by SDN, NFV
- Measurements at speeds over 100 Gbps
- Easy deployment of new monitoring tasks
  - without HW modifications
  - upon software application request
- Accelerates application-level processing

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