UNIVERSITÀ DEGLI STUDI
DI TRENTO

SECONOMICS

A quick analysis on data quality for risk evaluation.

11th Workshop on Economics of Information Security

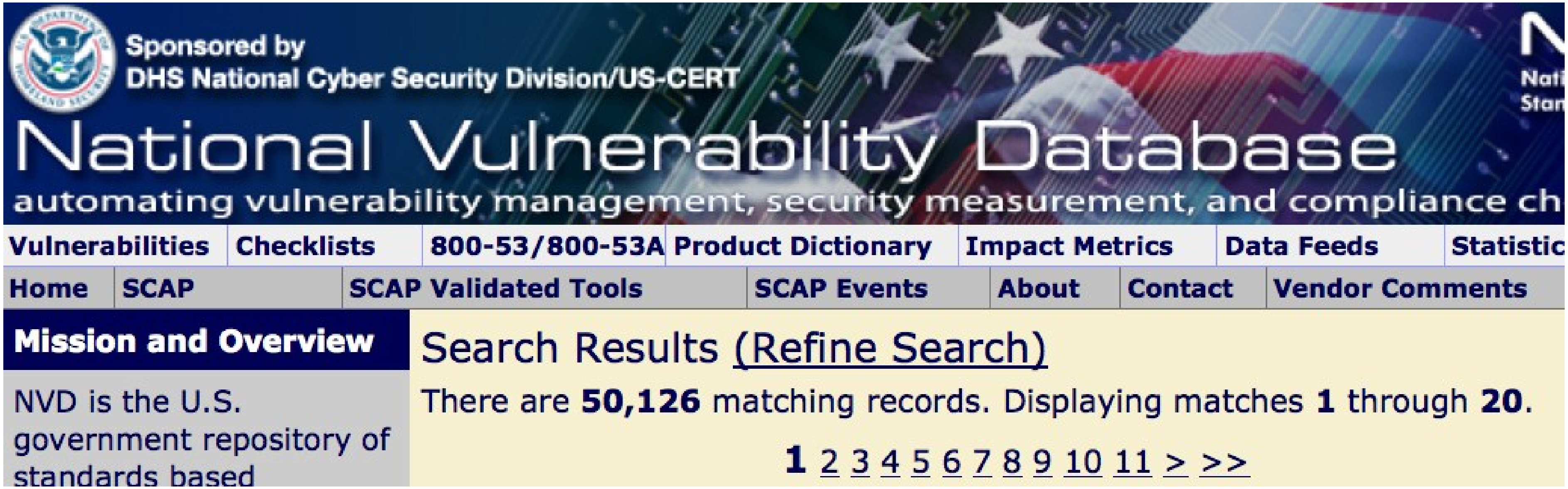
Rump Session

Luca Allodi, Fabio Massacci

25 June 2012, Berlin

Vulnerabilities and risk

- How many vulnerabilities in a system?
- How critical are they?
  - CVSS score



Sponsored by
DHS National Cyber Security Division/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance ch

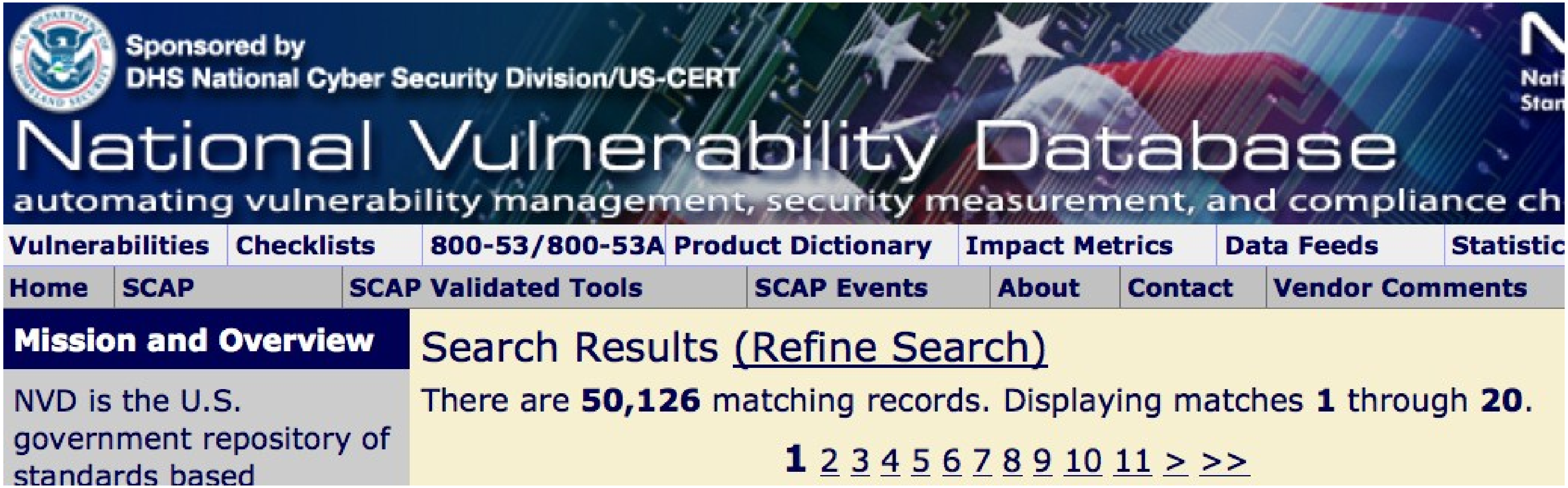
Mission and Overview

NVD is the U.S. government repository of standards based

Search Results (Refine Search)

There are **50,126** matching records. Displaying matches **1** through **20**.

Vulnerabilities and risk

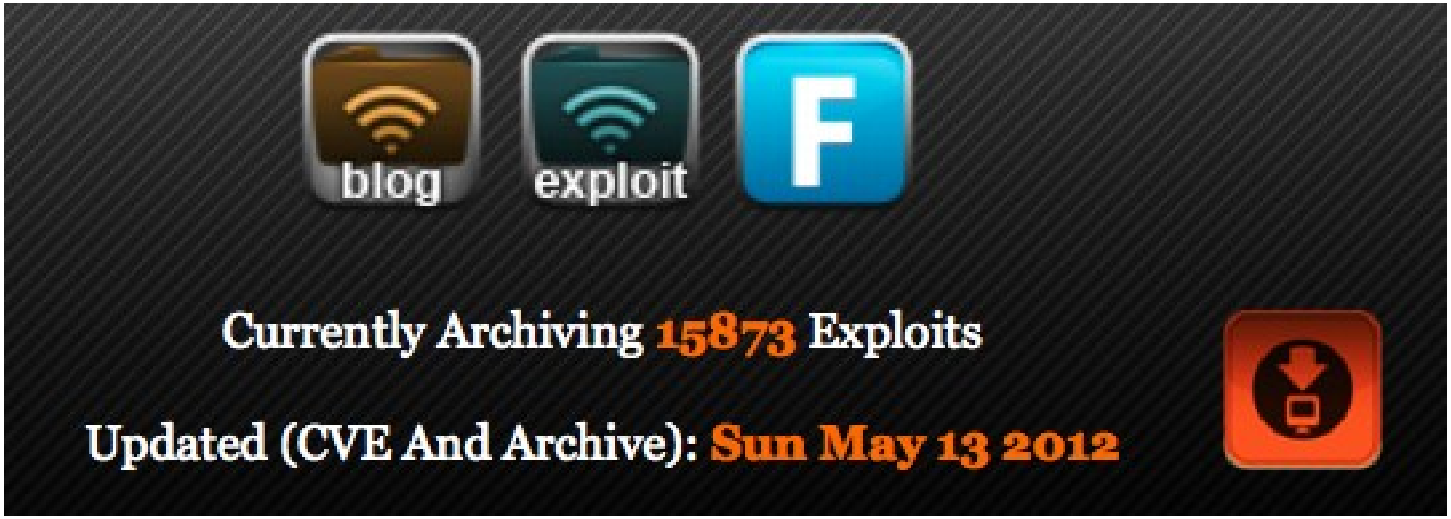


NVD is the U.S. government repository of standards based

Search Results (Refine Search)

There are **50,126** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 11 > >>

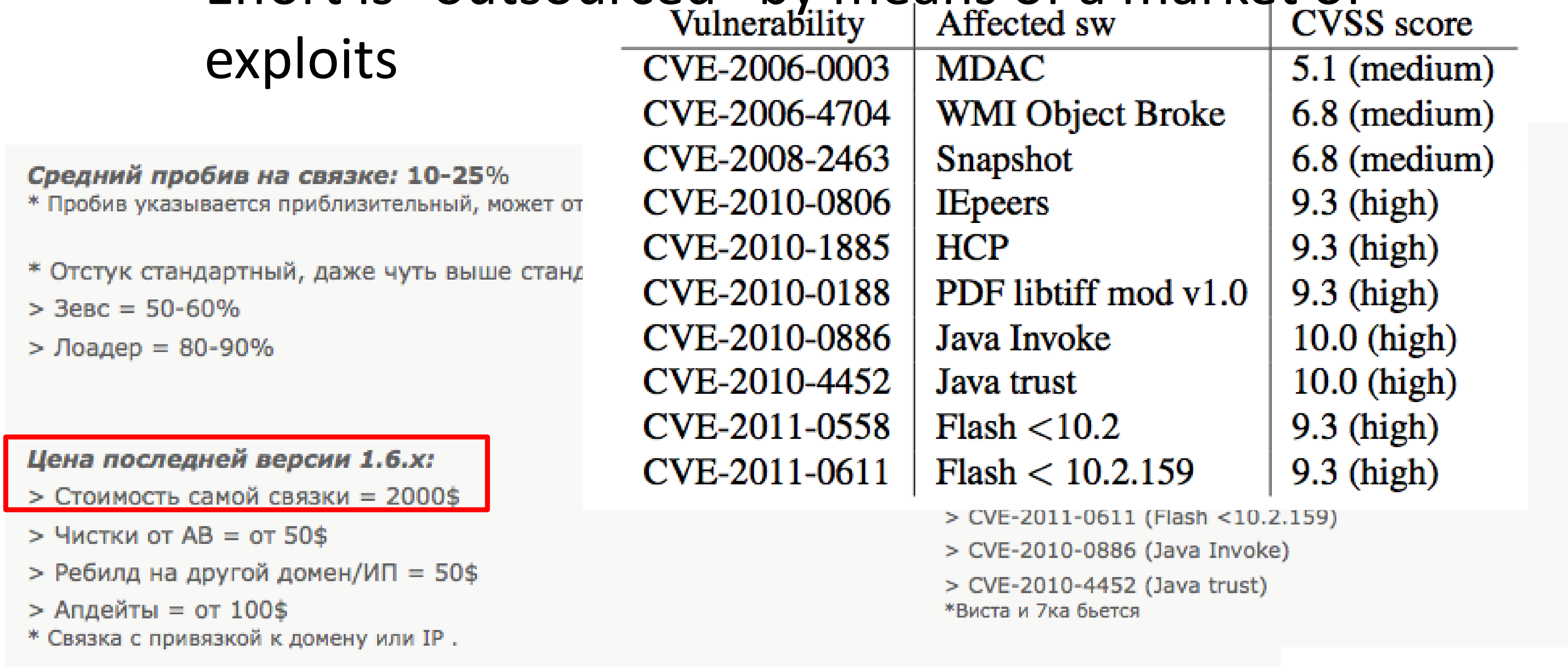


Currently Archiving 15873 Exploits

Updated (CVE And Archive): Sun May 13 2012

Exploits and attackers

- Writing a reliable exploit is not easy
  - Effort is “outsourced” by means of a market of exploits



Vulnerability	Affected sw	CVSS score
CVE-2006-0003	MDAC	5.1 (medium)
CVE-2006-4704	WMI Object Broke	6.8 (medium)
CVE-2008-2463	Snapshot	6.8 (medium)
CVE-2010-0806	IEpeers	9.3 (high)
CVE-2010-1885	HCP	9.3 (high)
CVE-2010-0188	PDF libtiff mod v1.0	9.3 (high)
CVE-2010-0886	Java Invoke	10.0 (high)
CVE-2010-4452	Java trust	10.0 (high)
CVE-2011-0558	Flash <10.2	9.3 (high)
CVE-2011-0611	Flash < 10.2.159	9.3 (high)

Средний пробив на связке: 10-25%
* Пробив указывается приблизительный, может от

* Отстук стандартный, даже чуть выше станд
> Зевс = 50-60%
> Лоадер = 80-90%

Цена последней версии 1.6.x:
> Стоимость самой связки = 2000$
> Чистки от АВ = от 50$
> Ребилд на другой домен/ИП = 50$
> Апдейты = от 100$
* Связка с привязкой к домену или IP .

> CVE-2011-0611 (Flash <10.2.159)
> CVE-2010-0886 (Java Invoke)
> CVE-2010-4452 (Java trust)
*Виста и 7ка бьется

Our baseline datasets

- National Vulnerability Database
- Exploit-db
- Symantec attack signature + threat explorer
  - Ground truth
- Direct exploration of the market (ekits)

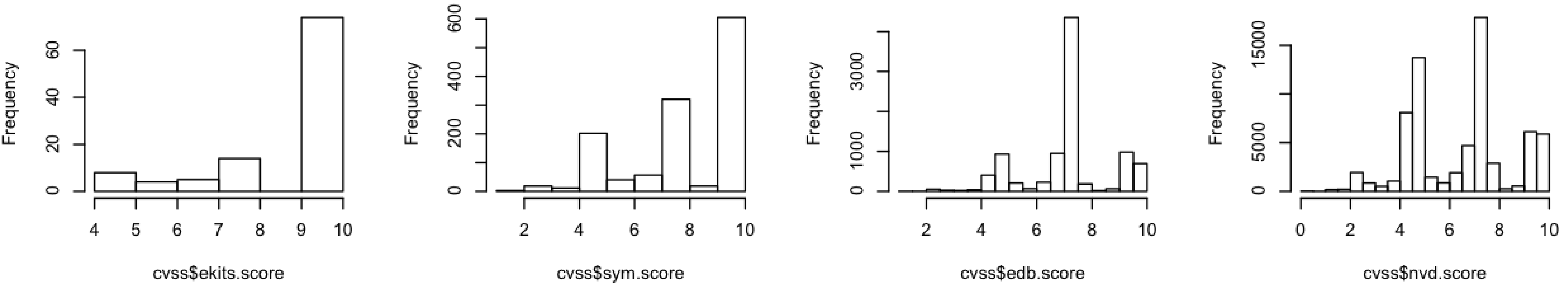
dataset	volume of CVEs
NVD	~50.000
EDB	~16.000
Symantec	~1300
Ekits	~100

Risk and databases

Probability that a vulnerability is an actual threat if it appears in a database

P(x Threat | in DB)	Ekits	Edb	NVD
Symantec	75.73%	4.08%	2.10%
Others	24.27%	95.92%	97.90%

Risk and databases (2)



	Ekits	**Edb**	**NVD**
P(x is threat | in DB and x.score >9)	81.08%	17.73%	6.37%
P(x is threat | in DB and x.score >6)	81.72%	4.78%	2.91%

Not all vulnerabilities are equally interesting
(and we don’t know why).

Thanks!

Any questions?