UNIVERSITY OF TRENTO - Italy
SECONOMICS
TENACE

Luca Allodi
Fabio Massacci
name.surname@unitn.it
https://securitylab.disi.unitn.it

Analysis of Exploits in the Wild

Or: Do CyberSecurity Standards make sense?

The world now

Current Cybersecurity Standards and Best Practices [1] make it clear:

1. **Fix all vulnerabilities**
2. **Use the CVSS Risk score to prioritise your work.**

Research Question #1

Is everything exploited, or do attackers have preferences?

Research Question #2

Is CVSS a good exploit marker?

Vulnerabilities: baseline

Dataset	Content
NVD	Universe of vulnerabilities
EDB	Exploits by security researchers
EKITS	Exploits by cybercriminals
SYM	Exploits deployed in the wild

Is everything exploited?

Figure 1 is a Venn diagram representation of our datasets. Areas are proportional to volume of vulnerabilities and colours represent HIGH, MEDIUM and LOW score vulnerabilities (red, orange, cyan respectively).

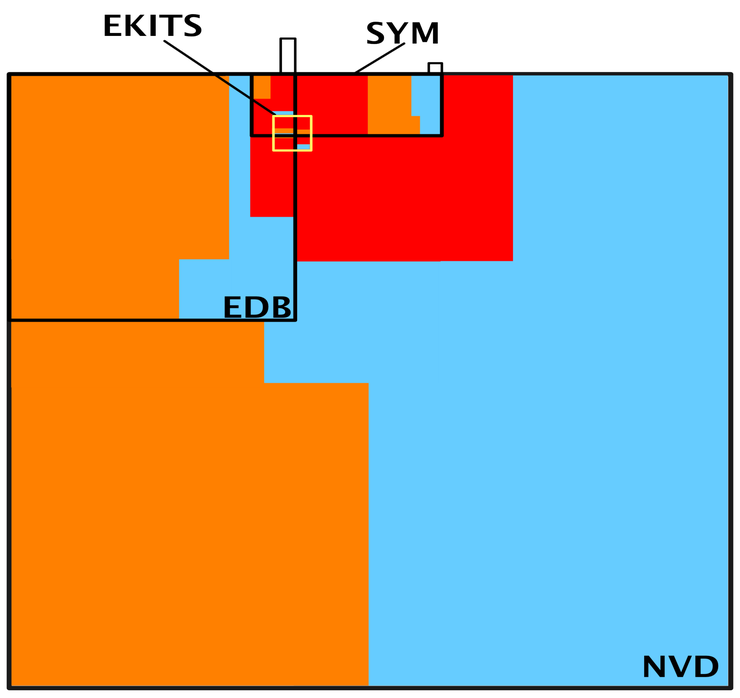

Fig. 1 Venn diagram of datasets

1. The greatest majority of vulnerabilities in the NVD are not included nor in EDB nor in SYM.

2. EDB covers SYM for about 25% of its surface, meaning that 75% of vulnerabilities exploited by attackers are never reported in EDB by security researchers. Moreover, 95% of exploits in EDB are not reported as exploited in the wild in SYM.

3. Our EKITS dataset overlaps with SYM about 80% of the time.

Conclusion 1. *Not only most vulnerabilities in NVD are never exploited, but most exploits in EDB are of no interest for the real attacker. Differently, if a vulnerability is traded in the black markets, it is most likely going to be attacked.*

Do attackers have preferences?

To further check for differences among datasets, we look at CVSS vulnerability *Complexity* and *Impact (Fig. 2)**.

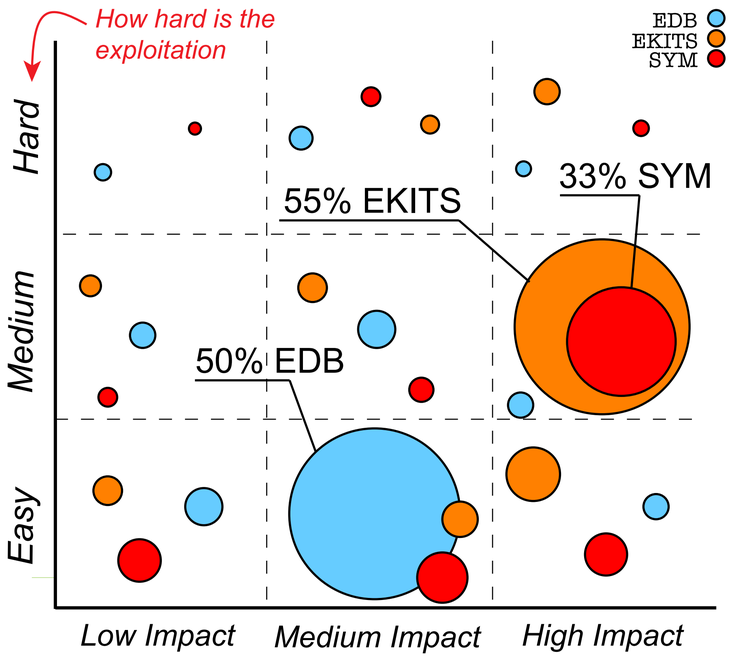

Fig. 2 Bubbleplot of vulnerability complexity vs impact

**Overlapping areas do NOT represent common vulns*

Attackers look at pay-offs in vulnerability exploitation (if difficult → high impact). Security reserachers seem to try to get as many "low hanging fruits" as possible by exploiting mostly easy vulnerabilities.

Conclusion 2. *Vulnerability databases can be misleadig with respect to what bad guys do. Conclusions in previous studies [2], [3] should be taken with a grain of salt.*

Is CVSS a good exploit marker?

In the medical domain, the sensitivity of a test is the conditional probability of the test giving a positive result when the illness is present. Its specificity is the conditional probability of giving a negative result when there is no illness.

$$\text{Sensitivity} = \Pr(\text{v.score} \geq 6 \mid \text{v} \in \text{SYM})$$

High Sensitivity = Patching is on target

$$\text{Specificity} = \Pr(\text{v.score} < 6 \mid \text{v} \notin \text{SYM})$$

High Specificity = Patching is economical

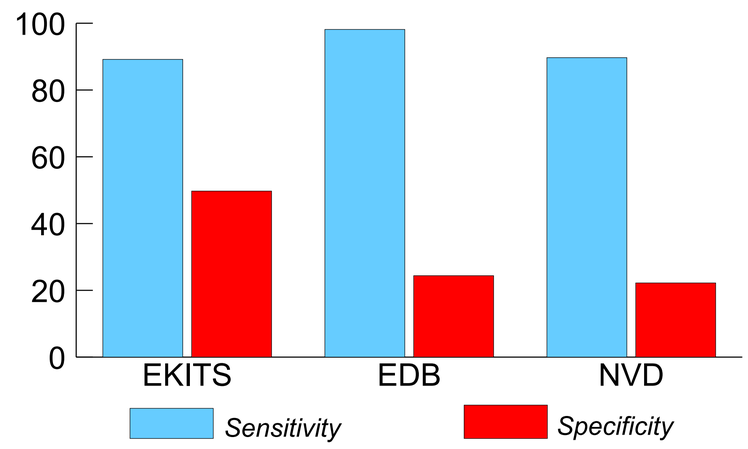

Fig. 3 Barplot of the Sensitivity and Specificity measures

Results are reported in Figure 3. The sensitivity of our samples is > 89%. On the other hand, the specificity is extremely low everywhere with a peak low in NVD and EDB at about 25%.
This means that 3 times out of 4, a vulnerability or an exploit marked as HIGH risk is not going to be exploited.

Conclusion 3. *The CVSS score is not a good predictor for exploitation. Policies relying on it to build sound strategies, such as US NIST Standard for assessing Cybersecurity Risk [1], may be widely sub-optimal.*

References

[1] S. D. Quinn, K.A. Scarfone, M. Barret, and C. S. Johnson. *Sp 800-117. guide to adopting and using the security content automation protocol (scap) version 1.0.* Technical report, 2010.

[2] M. Shahzad, M. Z. Shafiq, and A. X. Liu. *A large scale exploratory analysis of software vulnerability life cycles.* In Proc. of ICSE'12, pages 771–781. IEEE Press, 2012.

[3] S. Frei, M. May, U. Fiedler, and B. Plattner. *Large-scale vulnerability analysis.* In Proc. of LSAD'06, pages 131–138. ACM, 2006.

[4] P. Mell and K. Scarfone. A *Complete Guide to the Common Vulnerability Scoring System Version 2.0*. CMU, 2007.

[5] M. Rajab, L. Ballard, N. Jagpal, P. Mavrommatis, D. Nojiri, N. Provos, and L. Schmidt. *Trends in circumventing web-malware detection.* Technical report, Google, 2011.