Putting private and government CERT's to the test

Stefan Frei
stefan.frei@tik.ee.ethz.ch

Martin May
martin.may@tik.ee.ethz.ch

Swiss Federal Institute of Technology
Zurich, Switzerland
http://www.techzoom.net/risk

ABSTRACT

To be able to take notice of new vulnerabilities, business and enterprizes need accurate and validated information from a trusted source. CERT's and private sector service offerings provide such information through the publication of vulnerability advisories. The quality, quantity, and disclosure time of such advisories varies considerably between sources. By monitoring relevant security sites on 30-minute intervals for more than 18 months, we collected a unique dataset to compare CERT's and private offerings. In addition, we also collected data from well known exploit sites.

As an independent research institute, we present an unbiased analysis of the performance of CERT's and security information providers from the private sector. We show the evolution of the number of disclosures, number of references to CVE, the risk metrics used, and the timeliness of publication over the year, day of week and time of day. Correlating the advisories based on the CVE as a unique vulnerability identifier allows us to compare the advisory providers against each other. Further, we compare the advisory data with the rate of exploit publications. We find differences between the advisory providers and offer an interpretation. We revisit the vulnerability lifecycle with respect to our findings and examine their impact in the context of the full disclosure debate. We conclude that having multiple independent advisory providers is very important to the security society. Collectively, they serve as an efficient watchdog monitoring the (in)security scene, providing thread information in a usable format for businesses.

1. INTRODUCTION

In IT terminology, the term vulnerability is applied to a weakness in a system which allows an attacker to violate the integrity of this system. Vulnerabilities may result from weak passwords, software bugs, computer viruses or other malware, script code injection, or SQL injection. In spite of being recognized as a major thread for online businesses, it is difficult or impossible to completely prevent vulnerabilities. The strategy of today's security officers is therefore to cope with the potentially insecure environment by monitoring publications about new vulnerabilities and react rapidly to the identified threats. Consequently, key to successful defense against novel attacks is to get timely and complete information about emerging vulnerabilities.

Interesting questions to ask are then (i) where can the most appropriate information about vulnerabilities be found; and (ii) how can the timeliness and accuracy of security information be measured. In this paper, we try to give answers to these two questions. We identify the most well known sources where security advisories can be found and we will also present a methodology to measure the performance of these information providers.

As described in [2], the vulnerability life cycle is defined around the disclosure date of a vulnerability. The time of disclosure as the first date a vulnerability is described on a channel where the disclosed information on the vulnerability is (a) freely available to the public, (b) published by trusted and independent channel, and (c) has undergone analysis by experts such that risk rating information is included. Hence, for our analysis, we only consider vulnerabilities with a CVE entry. CVE stands for Common Vulnerabilities and Exposures and comprises a list of standardized names for vulnerabilities and information security exposures.

To address (i), we identified the most referenced sources of information about vulnerabilities. These are mainly CERT's and service offerings from the private sector. They all provide vulnerability information through the publication of advisories. In the remainder of this paper, we will call these information sources *Security Information Providers* (SIPs). As we will see later, the quality, quantity, and timeliness of such advisories vary considerably between sources. To address (ii), we present an analysis of the performance of the most prominent sources of CVE submissions. By monitoring relevant security sites on 30-minute intervals over a period of more than 18 months, we collected a unique dataset to compare CERT's and private offerings. In addition, we also collected data from well known exploit sites. This data is correlated with the content of the National Vulnerability Database (NVD) and the entries in the Common Vulnerability Enumeration (CVE) database. We will show the different working patterns

of the individual SIPs and compare them with the activities on the exploit archives. Our results indicate that while the SIPs follow classical daily and weekly patterns, the activities on the exploit side do not follow this trend. For timely delivery of vulnerability reports, additional efforts are necessary.

Concerning the performance of the SIPs in general, the good news is that most SIPs perform reasonably well. However, our data also indicate that one should not rely on only one information provider. To obtain the most timely and most complete vulnerability information, the security managers should at least use two SIPs.

This paper is structured as follows. Before describing the methodology used to assess the performance and quality of the SIPs, we first revisit in Section 2 the information provided in the CVEs as well as the process of collecting the required information. Then we introduce the information sources used throughout this document, the security information providers. In Section 3, we describe in detail how we collected the data as well as how the data is analyzed. The results of our comparison are presented in section 5, before we conclude this paper with a discussion and conclusion.

2. SECURITY INFORMATION SOURCES

2.1 Identification of Vulnerabilities

2.1.1 Common Vulnerabilities and Exposures (CVE)

In order to compare the flow of vulnerability information published in security advisories from different sources, we need a common understanding what a security vulnerability is. Counting or defining vulnerabilities is a delicate business that depends significantly on the parties involved (e.g., if something is considered *a bug, a feature*, or *a vulnerability* may differ if you talk to a researcher or the vendor of the affected software). For our study, we rely on the commonly accepted and widely used Common Vulnerabilities and Exposures (CVE) [9] description. CVE is a dictionary of common names for publicly known information system vulnerabilities. It is a *de facto* industry standard that has achieved wide acceptance in the security industry, academia, and a number of government organizations since its launch in 1999 [7]. CVE identifiers are now used in numerous information security products and services from around the world. From the original 321 entries in 1999, the CVE list has grown to over 30,000 entries as of April 2008. CVE is run by MITRE [11], a non-profit organization of the U.S government chartered to work in the public interest.

CVE provides the information security community with:

- a comprehensive list of publicly known vulnerabilities,
- an analysis of the authenticity of newly published vulnerabilities,
- and a unique identifier for each vulnerability

2.1.2 Creating a CVE identifier

A number of organizations in the information security community provide CVEs with vulnerability information that helps MITRE create new CVE identifiers. Since CVE does not rely on one single source, it has a better chance of identifying all publicly known security problems which then provides a more comprehensive set of vulnerability information for everyone. Note that all security data sources make their own decisions about which vulnerabilities they publish or include in their database. For example, they may exclude a security problem from their own database because it is not sufficiently proven to exist, there is incomplete information, or the problem is not important to the information provider's customers, etc.

The process of building the CVE list is divided into three stages: the *initial submission stage*, the *candidate stage*, and the *entry stage* [10]:

1. *Submission Stage*: CVE has a content team whose primary task is to analyze, research, and process incoming vulnerability submissions from CVE's data sources, transforming the submissions into candidates. The team is led by the CVE editor, who is ultimately responsible for all CVE content.
2. *Candidate Stage*: Candidates are normally created in one of three ways: (1) there are submissions from CVE's data sources; (2) they are reserved by an organization who uses it when first announcing a new issue (*e.g., big vendors or security companies get preassigned blocks of CVEs they use when publishing a new vulnerability*); or (3) they are created *out-of-band* by the CVE editor, typically to quickly create a candidate for a new, critical issue that is being widely reported. Candidates that pass the *editorial board* members review are accepted and entered into the CVE list (getting a CVE identifier assigned), if the candidate is rejected, the editor announce the reason for rejection.
3. *Entry Stage*: If the candidate has been accepted, the candidate is converted into an entry by changing its status from *candidate* to *entry* and removing the voting record. The updated entry is then added to the next version of the CVE list

For this research, we only consider vulnerabilities with a CVE [9] entry. Essentially, the decision on what counts as a vulnerability is delegated to the CVE ed-

itorial board which enjoys industry wide acceptance. Further, given the high acceptance of CVE we assume that any security issue *of relevance* will eventually get an CVE assigned.

Source	Referenced	Cumulated
Secunia (*)	15.36%	15.36%
SecurityFocus (*)	13.08%	28.44%
IBM ISS X-Force (*)	12.36%	40.80%
BugTraq	11.23%	52.03%
Miscellaneous	6.50%	58.53%
FrSIRT (*)	6.47%	65.00%
OSVDB	5.29%	70.29%
SecurityTracker (*)	4.05%	74.34%
Sreason	2.46%	76.80%
CERT (*)	2.28%	79.08%

Table 1: Top 10 most referenced sources in the CVE list (all entries by Jan 1st, 2008). 29,797 CVE entries contained 158,779 external references to 77 different sources. Sources we cover in this study are marked by (*)

2.1.3 National Vulnerability Database (NVD)

NVD [12] is the U.S. government repository of vulnerability data, indexed by CVE. NVD provides a detailed description of vulnerabilities, including a risk metric (High, Medium, Low, and CVSS) and software product information.

2.2 Security Information Providers (SIP)

Security companies and governments offer several widely used and highly valued announcement, alert, and advisory services for free. In this study, we compare the timeliness and completeness of security information provided by the most referenced information sources, namely *IBM ISS X-Force*, *SecurityFocus*, *Secunia*, *FrSIRT*, *SecurityTracker*, *SecurityWatch* and *US-CERT*. We call these sources *Security Information Providers* (SIP). In Table 1, we list the top 10 most referenced sources in the CVE list, which together account for 79% of all references.

2.2.1 IBM ISS X-Force (XF)

The ISS X-Force is the security research and development group of Internet Security Systems (ISS), since 2006 part of IBM. IBM ISS offers a range of security products and services, namely Managed Security Services (MSS), Intrusion Prevention Systems (IPS) and enterprise vulnerability scanner. IBM X-Force does active research of diverse products and technologies and ongoing surveillance within the security scene to identify new trends and malware. Since 1996 the X-Force publishes relevant discoveries as security advisories [4, 5] in their X-Force Database (XFDB). X-Force assigns one of three possible risk levels to vulnerabilities: High, Medium, Low.

2.2.2 SecurityFocus (SF)

SecurityFocus is a security news portal and purveyor of information security services since 1996. Since 1999 SecurityFocus is the owner of the well known Bugtraq [1] mailing list. In August 2002, Symantec [19] acquired SecurityFocus in full. Part of the purchase agreement was to keep SecurityFocus as an independent security portal. Symantec offers managed security services (MSS) and builds a range of security products, for end-users and enterprises (e.g., anti-virus, intrusion prevention systems). Security advisories and exploit material are provided to the public through the SecurityFocus vulnerability database. SecurityFocus assigns no risk rating but classifies the type of vulnerability. The Bugtraq mailing list was created in 1993 in response to the perceived failings of the existing Internet security infrastructure of the time. It started as a unmoderated mailing list for the full disclosure [21] of security vulnerabilities, to become moderated in 1995.

2.2.3 Secunia (Secunia)

Secunia [14], founded 2002 and based in Denmark, is an independent provider of vulnerability intelligence. Aside from gathering information from external sources, Secunia also conducts its own internal research. Secunia hosts the *Full-Disclosure* [6] security mailing list. Full-Disclosure is an unmoderated high-traffic forum for the disclosure of security information. The list was founded 2002 (after Symatec bought SecurityFocus) as an alternative to the moderated Bugtraq mailing list. Secunia assigns a five level risk rating to vulnerabilities: Not Critical, Less Critical, Moderately Critical, Highly Critical, and Extremely Critical.

2.2.4 FrSIRT (FrSIRT)

The French Security Incident Response Team FrSirt [3] is a private company based in southern France founded in 2003. FrSirt started delivering security and exploit advisories to the public in 2005. However, since early 2006 exploit information is only available as a payed service. FrSIRT provides a four level risk rating of the considered vulnerabilities.

2.2.5 SecurityTracker (SecTrack)

SecurityTracker [15], a vendor neutral security portal, is dedicated solely to reporting on security vulnerabilities. SecurityTracker monitors multiple public sources (vendor advisories and mailing lists) for security information but does conduct no own original research. It started operation in 2001. Security advisories published

by SecurityTracker are not risk rated, they classify the vulnerability impact with 13 classes.

2.2.6 SecurityWatch (SecWatch)

SecWatch [17] provides the security community with vulnerability and exploit information since 2004. SecWatch is currently (April 2008) considering the sale of this site and related services. SecWatch provides a five level risk rating with security advisories.

2.2.7 US-CERT (Cert)

Worldwide, there are more than 250 organizations that use the name *CERT* or a similar name that deal with cyber security. The first of these types of organizations is the CERT Coordination Center (CERT/CC), established at Carnegie Mellon University in 1988. The US Computer Emergency Readiness Team (US-CERT) [20] is the operational arm at the Department of Homeland Security (DHS) of the US. It is a public-private partnership that publishes information about vulnerabilities as vulnerability notes. Vulnerability notes include technical descriptions of the vulnerability, as well as the impact, solutions and workarounds, and lists of affected vendors. A number between 0 and 180 assigns an approximate severity to the vulnerability. We use the vulnerability notes of US-CERT in our study.

2.3 Exploit Archives

To shed a light on the "other side" of the security industry. we also include three well known exploit archives in our study for comparison. Correlation of exploit information with CVEs is inherently more difficult (there is no CVE for a zero-day exploit, and published exploits are usually not maintained or updated in order to include a CVE later). We only use these sources for a comparison of the daily and weekly working pattern. We monitored *Milw0rm* [8], *Packetstorm* [13] and *SecurityVulns* [16] for new exploits.

3. METHODOLOGY

3.1 Overview

Our methodology to measure the performance of security information providers (SIP) consists of three major phases, namely (1) to monitor the appearance of new advisories with 30 min intervals, (2) to download and parse all known advisories from know SIPs, and (3) to correlate the information gained in phases (1) and (2). In Section 2, we listed the SIPs and exploit archives included in our study. As mentioned in Section 2, we only consider advisories from these sources when they have a CVE attached.

3.2 Phase 1 - Monitoring

We wrote a web spider that downloads and parses the *entry page* of the specified web sites every 30 minutes since August 2006. The entry page is the page where new advisories (or exploits) and other news are listed by the SIP. To identify new advisories, the parser extracted all URLs found in the entry page and compared it to the list of URLs from the last download. Newly found URLs that match the format of URLs to security advisories (or exploits) are timestamped and logged for later analysis and correlation. In this first phase, we only record *new URLs to advisories*. That means, we did not instantly download the advisory (or exploit) itself (see *Phase 3* for more details).

3.3 Phase 2 - Collecting all advisories

At a later time, we spidered and parsed all the advisories from these SIPs. This includes advisories published before our monitoring spider started operation in August 2006.

A complete list of advisory (or exploit) URLs to be downloaded was built from several sources:

1. URLs found by the monitoring spider.
2. References in the National Vulnerability Database NVD [12] and the CVE [9] archive documents.
3. References found in the *Archive* section of the SIP where they host lists to all their past advisories.
4. Cross references found in the advisories of other SIPs.
5. Enumeration of advisory URLs in case the format followed a predictable pattern (*e.g. sequential or date based IDs in the URL*).

After the download of these advisories representing more than 200,000 documents, our parser extracted the following information (if available) from the content of these advisories:

1. The SIP specific identification of the advisory (*e.g., the BID-*99999 *for SecurityFocus' Bugtraq ID, SA*99999 *for Secunia Advisory, ..*).
2. The risk rating of the vulnerability.
3. The disclosure date (publication date) of the advisory.
4. The CVE, or list of CVEs of the advisory.
5. URLs of references to other security sites.

Table 2 lists the total number of advisories found per source and year since 2004. Note that *FrSIRT* started operation only in 2005. The date was taken from the content of the respective advisory.

An advisory may contain more than one CVE entry. Therefore, we list in Table 3 the number of **unique** CVEs found in all advisories. In Table 4, we list the number of unique CVEs tracked by our monitoring spider in 2007 per source.

Source	2007	2006	2005	2004
ISS	6,312	7,060	4,719	2,810
SF	4,941	5,564	3,500	2,368
Secunia	9,231	10,794	8,523	4,150
FrSirt	6,337	8,311	3,072	-
SecTrack	1,793	2,389	1,961	1,555
SecWatch	1,291	1,343	1,523	536
Cert	340	505	315	350
NVD	**6,532**	**6,600**	**4,928**	**2,450**

Table 2: Number of all published advisories (including those without a CVE) per source and year.

Source	2007	2006	2005	2004
ISS	6,022	6,672	4,401	2,600
SF	4,797	5,386	3,302	2,303
Secunia	4,535	5,754	4,022	2,063
FrSIRT	3,842	5,019	2,282	-
SecTrack	1,665	2,162	1,840	1,488
SecWatch	1,098	1,126	1,216	429
CERT	330	480	299	321
NVD	**6,532**	**6,600**	**4,928**	**2,450**

Table 3: Number of *unique CVEs* covered by advisories of given source and year.

Source	Advisories
ISS	2,065
SF	4,714
Secunia	4,182
FrSirt	3,544
SecTrack	1,580
SecWatch	1,960
Cert	320

Table 4: Number of advisories with CVE detected by our monitoring spider in 2007.

3.4 Phase 3 - Correlation

The correlation of the information from Phase 2 is a two step approach: (1) proper identification of vulnerabilities across different sources; (2) correlation of vulnerabilities with our monitoring data:

3.4.1 Identification of vulnerabilities

For this study, we only use vulnerabilities that have a CVE assigned. In most cases, the CVE information is found in the advisory itself (where the advisory refers to the corresponding CVE). However, in many instances, the CVE reference was entered well after the initial release of the respective advisory (*e.g., the description of a new vulnerability was published with an advisory. Then, several days or weeks later, a CVE was assigned to this vulnerability, the original advisory was updated, and a CVE reference was added*). Therefore, we separate *Phase 1* and *Phase 2* of this study.

In *Phase 1*, we collect timestamps of the first appearance of advisories using short intervals. In *Phase 2*, at a later time, we spider the advisory to capture cases where CVEs were assigned later. Some SIPs were found not to update (add CVE) their advisories on a regular basis. To capture these cases, we used references in NVD and CVE documents (where a CVE is always assigned by definition) for the correlation of CVE to advisory *e.g., over 40% of all the CVEs of SecurityFocus were assigned this way.* The output of this step is a set of CVEs with several advisories assigned from different sources. The correlation through CVE allows us to compare advisories from multiple sources relating to the same vulnerability.

3.4.2 Correlation with monitoring data

We correlate the timestamps collected in Phase 1 with the advisories and CVEs found in the previous step after normalization of all URL cross-references. Potentially, this gives us accurate timestamps for all advisories released after we started our monitoring agent in August 2006. However, our analysis revealed that not all advisories of these sources where first published in the entry page we monitored. This explains the difference in the number of advisories found in Phase 2 and the number of advisories available for high resolution timing comparison. For example, IBM ISS X-Force published more advisories than we captured with our spider, partly because of changes in their website since the purchase by IBM in late 2006.

4. DISCLOSURE STRATEGIES

4.1 Disclosure Information

We first examine the completeness of security information obtained with a single source or with a combination of security information sources. We extend the counts from Table 3 and include combinations of two SIPs (*IBM ISS X-Force, SecurityFocus, Secunia, FrSirt*) for the year 2007. In 2007, a total of 6,532 unique CVEs were released according to the NVD (based on the NVD publication date). Table 5 shows that the best coverage one can get from a single source is 92% of the CVEs released that year. However, when the information of two providers are combined, we exceed 95% and even get up to 99% completeness. We conclude that for a complete coverage of security information, it is advisable to consult at least two different SIPs. In

Source	% ISS	SF	Secunia	FrSIRT
ISS	6,022 92%	6,264 95%	6,437 99%	6,416 98%
SF		4,797 73%	5,802 89%	5,637 86%
Secunia			4,535 69%	5,042 77%
FrSirt				3,842 59%

Table 5: Number and percentage of unique CVEs covered by any combination of two sources. Total number of CVEs from NVD 2007.

2007, this would have been the combination of ISS and Secunia.

4.2 Working patterns

We first look at the distribution of advisory and exploit publications by the hour during the day, and by the day during the week. We examine the sources presented in Section 2, namely seven SIPs and the three exploit archives *Milw0rm*, *Packetstorm*, and *SecurityVulns*. In Figure 1, we plot the distribution of the disclosure time during the 24 hours of the day. All time information is normalized to UTC. For all but *SecurityTracker* and *SecurityVulns* we find a clear pattern of working and non working hours. Presumably, these patterns are determined by the day/night periods in different timezones. We assume that the rather uniform distribution found in the hourly distribution of *SecTrack* and *SecurityVulns* is a result of automatic information retrieval tools. Note here also that *SecTrack* does not perform its own research. We assume that the peak at 11h UTC in in the hourly distribution of *SecurityVulns* is the result of a daily batch update of the sites content. Note also that *IBM ISS X-Force*, *SecurityFocus*, *SecurityWatch*, and *CERT* operate in US timezones. *Secunia* and *FrSIRT* operate in Europe while *PacketStorm* appears to operate or receive its exploit contributions from Far East timezones.

In Figure 2, we examine the weekly distribution of advisory and exploit disclosures of the same sources. We find that all security information providers follow a clear workday/weekend pattern of disclosures, with few or no disclosures during the the weekend. This contrasts to the disclosure of exploit material. *Milw0rm*, *Packetstorm*, and *SecurityVulns* show an almost uniform disclosure rate throughout the week. When new exploits being released over the weekend, there will be likely a longer delay until the public has access to this information through the free services offered by SIPs.

5. PERFORMANCE COMPARISON

In this section, we examine the timing of the publication of security advisories between the sources listed in Section 2. For all CVEs published in the NVD in 2007, we noted the time of disclosure of each SIP covering these vulnerabilities. For only few CVEs we found no reference to a SIP. However, the majority of CVEs were covered by more than one SIP as shown in Table 5. From this list, we selected only entries with at least two SIPs reporting a given vulnerability. We then evaluate the time the first advisory was published and the time difference of all other SIPs to this minimum time. In Figures 3 and 4 we plot the percentage of advisories disclosed by a given source within time t after the first disclosure.

Sources N	All CVEs	CVEs with $N > 1$
1	2946	0
2	1908	1908
3	2058	3966
4	1860	5826
5	1080	6906
6	489	7395
7	115	7510

Table 6: This table lists the number of CVEs that were covered by security advisories of N different sources, and the cumulated number of CVEs covered by $N > 1$ sources. For the performance analysis we only used entries with $N > 1$

In Table 6, we list the number of CVEs that where covered by a given number of SIPs. This list only includes advisories that got logged by our monitoring spider as described in Section 3.

5.1 Short-Term Analysis

In Figure 3 (Color plots are available online [18]) , we show the short term dynamics within 48 hours after the first SIP disclosed a given vulnerability. *Secunia* is in 48% of the vulnerabilities the first SIP to disclose a vulnerability, closely followed by *SecurityFocus* with a 45% share. Note that the first publication of a vulnerability can be attributed to more than one SIP at the same time when published simultaneously [1]. All SIPs have a share of at least for 20% "first to report vulnerabilities", except *SecWatch* with only 1%.

We also measured the percentage covered by these SIPs 24h after the first disclosure to account for the time difference between timezones around the world. The effect of different timezones is visible through the low

[1]the sets of vulnerabilities per source do partially overlap, several SIPs can report a vulnerability at the same time

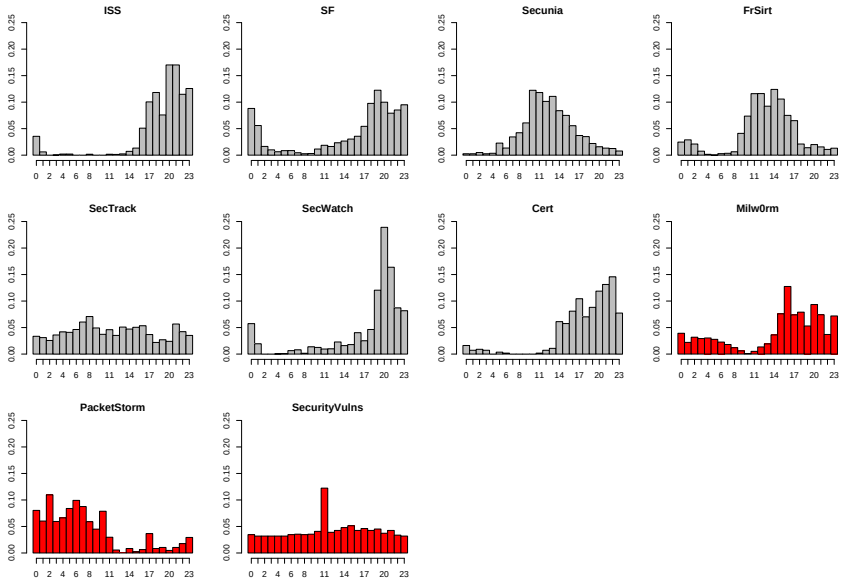

Figure 1: Distribution of advisory and exploit disclosures by hour of the day, timezone UTC.

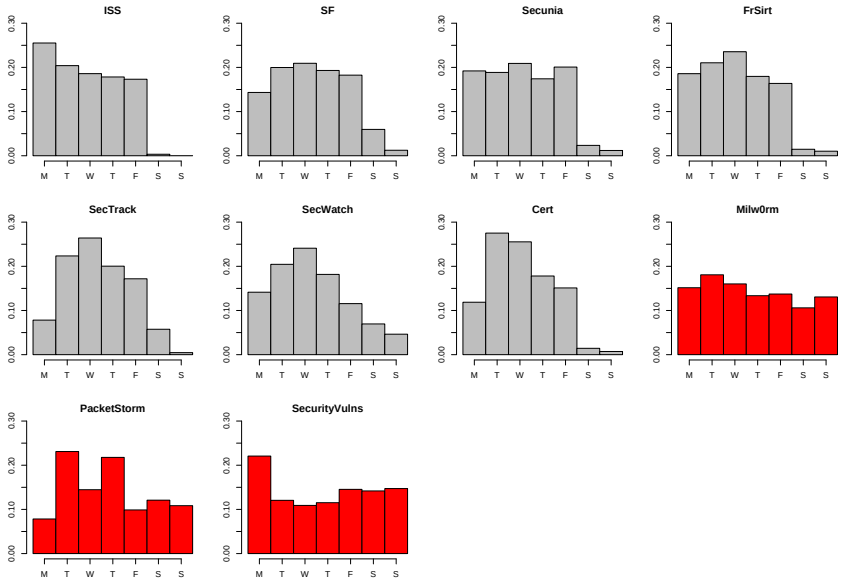

Figure 2: Distribution of advisory and exploit disclosures by day of week.

frequency modulation of the different curves' slopes. At 24h, *SecurityFocus* and *IBM-ISS* lead with about 85% closely followed by *SecTrack* and *Secunia* with about 80%. *SecWatch* and *CERT*, cover a comparably low number of vulnerabilities (Table 6) and fall behind with 63% and 54% share at 24h.

Many of the SIPs operate with the goal to provide vulnerability information as early as possible. We now discuss briefly the prerequisites to become a early vulnerability information provider. To be the first to disclose a vulnerability, a SIP has to do a combination of the following:

- Conduct own original research. This gives the SIP a monopoly on the vulnerability information until the public disclosure. The public disclosure shall be coordinated with the release of a patch or fix by the vendor of the affected software.
- A SIP has to efficiently monitor know sources of vulnerability information, such as security mailing-lists and underground sources, and other SIPs.
- Managing security operations (Managed Security Services) for a large customer base (Anti virus, Intrusion Prevention Systems) provides a SIP with

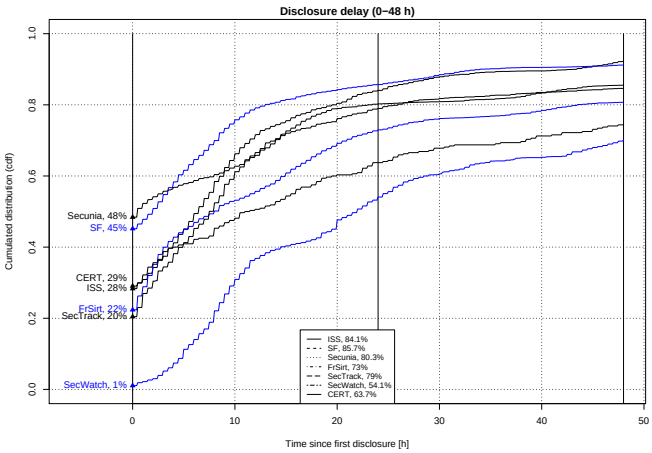

Figure 3: Percentage of advisories released within 48 hours of the first publication of the vulnerability. Color plots are available online .

first hand samples of new malware for analysis.

- Vulnerability market: a SIP buys vulnerabilities and new exploit material. This gives the SIP a de facto monopoly on the vulnerability information until the public disclosure through coordination with the affected vendor.

Generally, we observe high dynamics in the publication of security advisories between different SIPs within 24h of the first reporting a vulnerability. Also, with one exception, all SIPs are first contributors and there is no single source everyone else copies from. We conclude that we observe a healthy and highly competitive market between the different of security information providers. This market ensures that the public has access to timely and accurate security information. This diversity and choice of source is preferred over a single government sponsored agency providing security information. We further see that analyzing fewer vulnerabilities does not mean to be faster.

Source	$t = 0h$	$t \leq 24h$	$t \leq 30d$
ISS	29%	84%	98%
SF	45%	86%	98%
Secunia	48%	80%	97%
FrSirt	22%	73%	94%
SecTrack	20%	79%	94%
SecWatch	1%	54%	94%
CERT	29%	63%	93%

Table 7: Percentage of vulnerabilities released by a given SIP within 0h, 24h, or 30d after the first SIP published an advisory.

5.2 Long-Term Analysis

Figure 4 shows the long term dynamics up to 60 days after the first disclosure. The top performers among the observed SIPs publish 90% of their advisories within 48h after the first disclosure of a vulnerability.

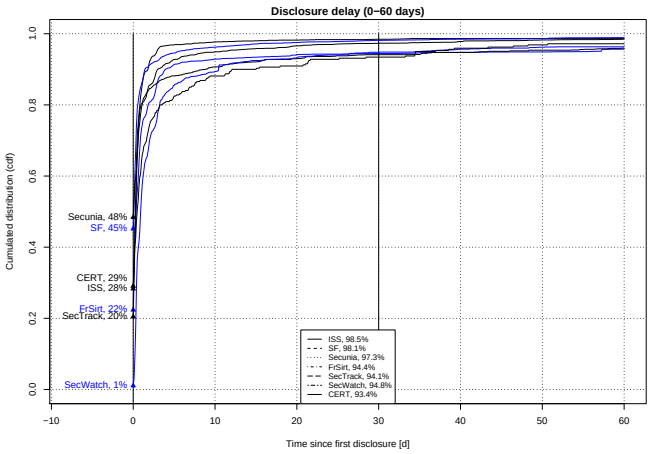

Figure 4: Percentage of advisories released within 30 days of the first publication of the vulnerability.

On the other side of the spectrum, the slowest SIPs requires more than 15 days to to achieve the same percentage of completeness. One final remark on the risk rating of the vulnerabilities. Further analyzing the disclosure dynamics indicates that the risk rating of a vulnerability does not affect the timeliness of disclosure.

6. DISCUSSION AND CONCLUSION

In this paper, we identified and queried the performance of the most referenced security information provides. Therefore, we collected and analyzed over 200'000 security and exploit advisories from numerous sources. To compare their performance, we correlated the individual advisories with the CVEs published in the national vulnerability database.

The first contribution of this paper is the methodology used to perform this comparison. It requires an intimate knowledge of the security environment and the processes of the vulnerability disclosure.

With the help of the timeliness and completeness evaluation, we have seen that the best known security information providers operate in an competitive environment. When combined, the information provided covers 99% of the vulnerabilities reported within 24 hours.

Considering the timeliness of the information provided, one sees that no single provider dominates the landscape. That means that we have multiple sources that independently monitor the (in)security scene in an efficient and complementary way. Besides the security

information provider performance, we also monitored three well known public exploit archives. Our data indicates that while SIPs follow a regular weekly pattern of activity, the publication rate of exploits does not decrease over the weekend. We have shown that with the combination of multiple security information provides from different timezones, one achieves a very complete and timely information feed.

The important finding of our work is that the competitive environment in which the security providers operate, is the best guarantee for unbiased and timely vulnerability information accessible by the public.

We plan to continue our effort in this field and hope to provide an ongoing monitoring of the performance of the most prominent security information providers.

7. REFERENCES

[1] Bugtraq. Bugtraq Security Mailing List. `http://www.securityfocus.com/archive/1`.

[2] S. Frei, M. May, U. Fiedler, and B. Plattner. Large-scale vulnerability analysis. In *LSAD '06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*, pages 131–138, New York, NY, USA, 2006. ACM.

[3] FrSIRT. FrSIRT. `http://www.frsirt.com`.

[4] IBM Internet Security Systems. X-Force Advisory. `http://www.iss.net`.

[5] IBM X-Force. IBM X-Force Disclosure Guidelines. `http://documents.iss.net/literature/vulnerability_guidelines.pdf`.

[6] John Cartwright. Full Disclosure Mailing List. `http://lists.grok.org.uk/full-disclosure-charter.html`.

[7] R. A. Martin. Integrating your information security vulnerability management capabilities through industry standards (CVE & OVAL). *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, 2:1528–1533 vol.2, 5-8 Oct. 2003.

[8] Milw0rm. Milw0rm Exploit Archive. `http://www.milw0rm.com`.

[9] MITRE. Common Vulnerabilities and Exposures (CVE). `http://cve.mitre.org`.

[10] MITRE. How We Build the CVE List. `http://cve.mitre.org/cve/identifiers/build.html`.

[11] MITRE. MITRE Corporation. `http://www.mitre.org`.

[12] NVD. National Vulnerability Database. `http://nvd.nist.gov`.

[13] Packetstorm. Packetstorm Security. `http://packetstormsecurity.org/exploits50.html`.

[14] Secunia. Vulnerability Intelligence Provider. `http://www.secunia.com`.

[15] SecurityTracker. SecurityTracker. `http://www.SecurityTracker.com`.

[16] Securityvulns. Computer Security Vulnerabilities. `http://securityvulns.com/`.

[17] SecWatch. SecurityWatch. `http://www.secwatch.org`.

[18] Stefan Frei, Martin May. Online repository of plots. `http://www.techzoom.net/publications`.

[19] Symantec. Symantec. `http://www.symantec.com`.

[20] US-CERT. US-CERT. `http://www.us-cert.gov/aboutus.html`.

[21] Wikipedia. Full Disclosure. `http://en.wikipedia.org/wiki/Full_disclosure`.