

SECURITY THREATS AND TRENDS

JULY 2007

SECODE AB

Secode helps companies and organizations gain insight, competence and thereby control over their operations from a complete IT security perspective. We deliver proactive and perpetual vigilance within two areas: 24/7 Managed Security Services and Security Consulting.

The Company was originally founded in 1986 as System Sikkerhet A/S, in Arendal, Norway. In year 2000, Secode AB was founded in Sweden and started its 24/7 Managed Security Services and Security Consulting. The two companies merged in January 2004, thereby forging the leading Digital Security Company in the Nordic region. In March 2006 the Finnish IT-security company Netsol OY (founded in 1996) was merged into Secode. From the first of January 2007 Secode has established sales-offices in both Denmark and The Netherlands and delivers IT-security services to customers in these countries as well. Secode helps many customers in private and public sectors, from seven different locations, using close to 85 security specialists. These specialists have long experience from building large computer networks and/or up-to-date IT security competence. Secode AB today has more than 100 employees.

All this together makes Secode the leading Northern European Digital Security Company within Managed Security Services combined with IT-Security Consultancy Services.

SUMMARY

The traffic level has increased quite a lot this period. In comparison with July last year we can say that the increase is strong. June 12th there was an increase in the number of searches towards the service MS SQL. This is probably due to the release of a new MS SQL Server version. Among countries of origin we now see a clear change. Multiple East-European and South-American countries have now entered the list.

The 'Focus of the Month' covers the zero-day attack phenomena.

TABLE OF CONTENTS

INTRODUCTION	4
THREAT LEVEL	5
RECONNAISSANCE ATTACKS JUNE 2007	5
TYPE OF RECONNAISSANCE ATTACKS.....	6
RECONNAISSANCE ATTACKS PR COUNTRY	7
INTERNET WORMS AND SPAM	8
ALERT STATISTIC	9
HANDLED ALERTS.....	9
REPORTED INCIDENTS.....	10
FOCUS OF THE MONTH – ZERO-DAY ATTACK.....	11
DEFINITION.....	11
EXAMPLES.....	12
CHALLENGES.....	12
SOURCES	13

INTRODUCTION

This report is based on three main parts; Threat level, Alert Statistic and Focus of the Month.

Threat level is a presentation of what threats organizations are exposed to through their Internet connection. In this threat evaluation, reconnaissance attacks from the Internet against customers of Secode are analyzed and presented.

Alert Statistic is based on alerts from Secode's IDS and IPS tools. An alert appear when a sensor recognizes network traffic that fit the implemented signatures/filters, and in these cases alerts will be transferred to Secode SOC (Security Operation Center). All alerts, both false and genuine, are manually handles by analysts at Secode.

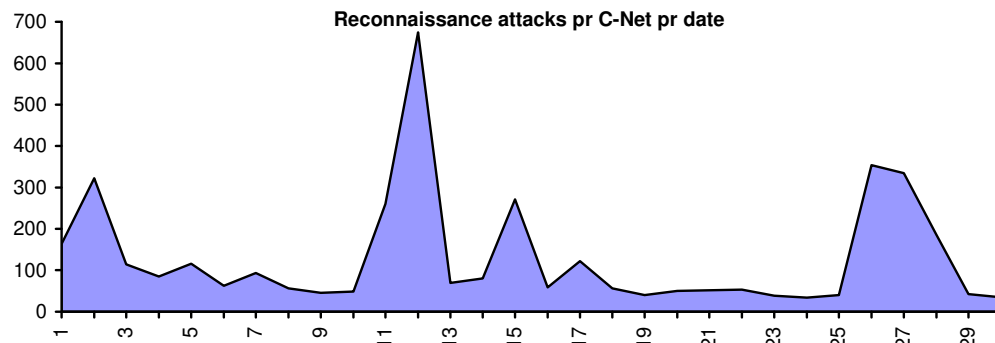
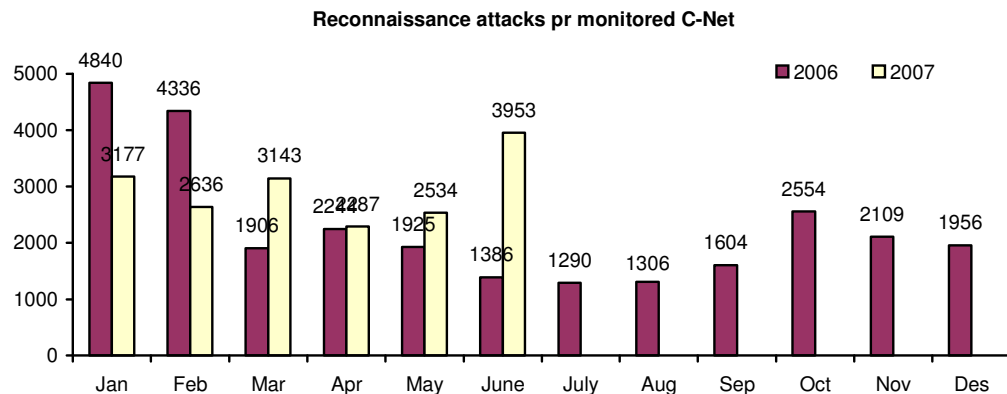
Focus of the Month is an article about relevant topics within IT Security. These might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

THREAT LEVEL

Due to high activity level, Internet worms and spamming are handled in a separate subchapter; "Internet worms and Spam", and are excluded from the other charts in this chapter.

RECONNAISSANCE ATTACKS JUNE 2007

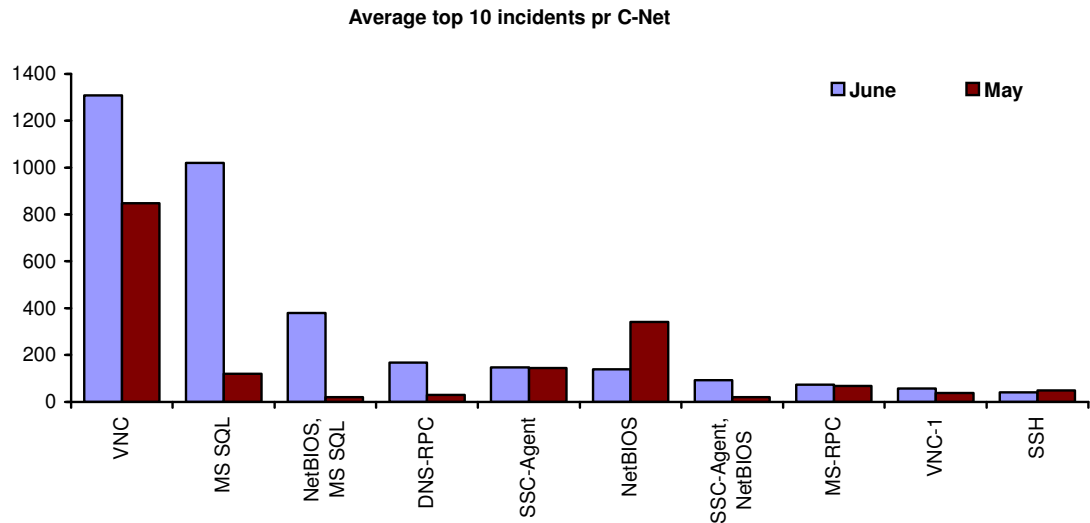
The statistics below gives an overview of the average number of reconnaissance attacks per network under surveillance. However, the activity level may vary from one network area to another. Despite these variations in the total activity level, we (mostly) register the same kind of attacks in different network areas.



In this period there has been a strong increase in the number of reconnaissance attacks in comparison with the tendency we saw a year ago. As you may see in the graph, there has been most traffic around June 12th. We also see some increase in the end of the month. There is no single attack behind these peaks, but rather reconnaissance attacks from all over the world towards several net ranges.

TYPE OF RECONNAISSANCE ATTACKS

The diagram below contains a summary of the most common reconnaissance attacks during the last two months. The diagram does not separate scans for one single service from combined scans for several services.



Scans for VNC are still the number one service, not unexpectedly since several RealVNC vulnerabilities have become known the last couple of months. The last vulnerability makes it possible to exploit the authentication protocol and then enter the server.

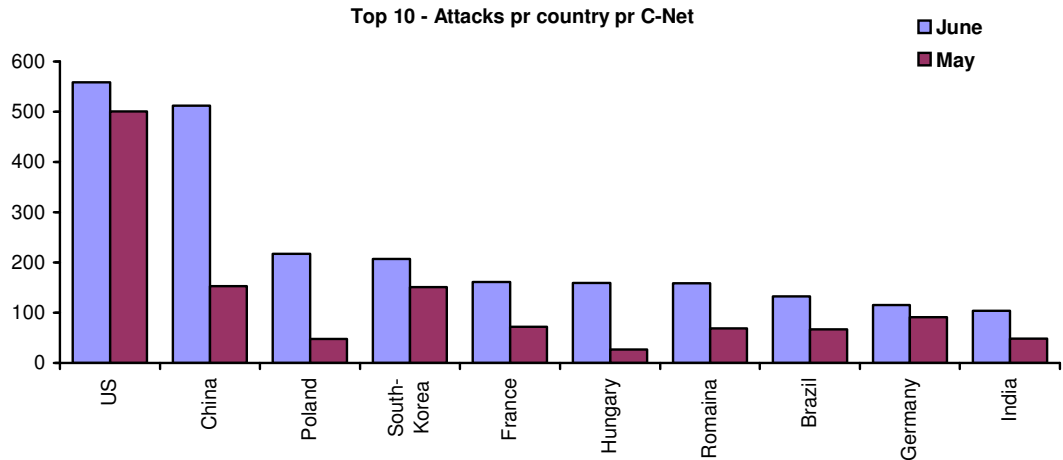
The biggest change for last period is however the increase in traffic towards MS SQL. Scans towards this service is the source of most of the traffic around June 12th, and this is most likely connected to the fact that Microsoft released their CTP (Community Technology Preview) version of their SQL Server 2008 this day.

We have registered quite an increase in the traffic towards port 1025 (DNS-RPC) as well. For this service, as for the other services, new vulnerability has been released during the last couple of month. This service is exposed to Rinbot worms searching for the ports, and new version of Rinbot worms surfaces regularly, only with small variations.

NetBIOS is the only service on the top 10 list which have decreased this period. The increase towards the other services is due to an overall increase in Internet traffic.

RECONNAISSANCE ATTACKS PR COUNTRY

The malicious activity in the statistic below is mainly automated attacks, which comes from infected computers (e.g. Internet worms or viruses). This means that most of the attacks are not directly aimed.



Among the countries of origin there are strong differences from last period as well. The most noticeable difference is that there are many “new” countries on the list.

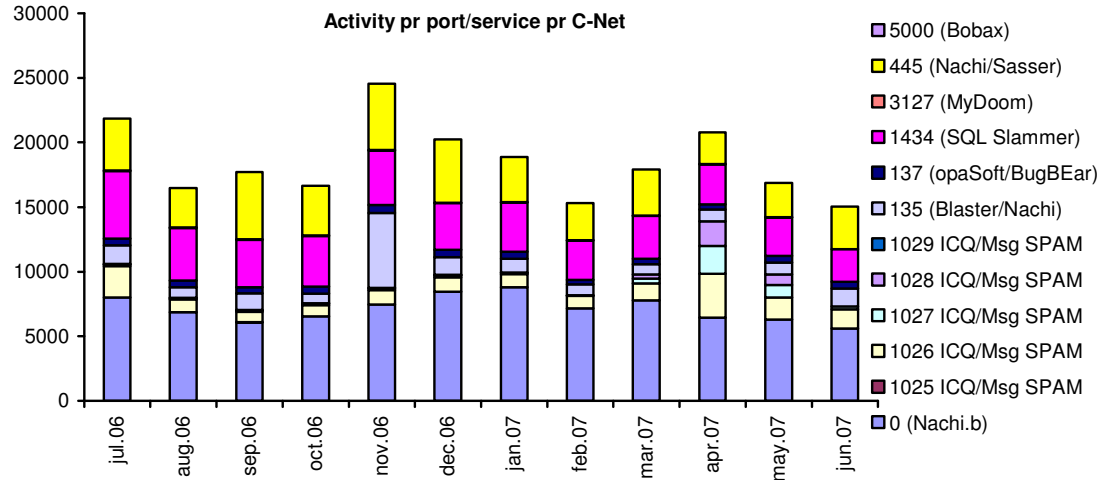
China have had the strongest increase this period, and are now closely to the same level as the US. In several c-net segments we have seen that China has surpassed the US level. Most of the traffic from China is towards MS SQL.

We also see quite a lot of increase from Eastern-Europe, as we mentioned in the previous Threats and Trends. This trend does not seem to turn in a while. India and Brazil have not been on the list previously, at least not during the last year.

The US is this month followed by China and Poland.

INTERNET WORMS AND SPAM

Because of a high level of activity against certain services, such traffic is presented in separate statistics. This applies for services most frequently targeted by Internet worms and spamming attempts.



Once again there is a reduction in worms and spam activity. It is not unusual that when there is an increase in the level of reconnaissance attacks there is a reduction in spam and worm activity. There has been a decrease towards all services, with exception of port 137 and port 445, which have had a slight increase.

ALERT STATISTIC

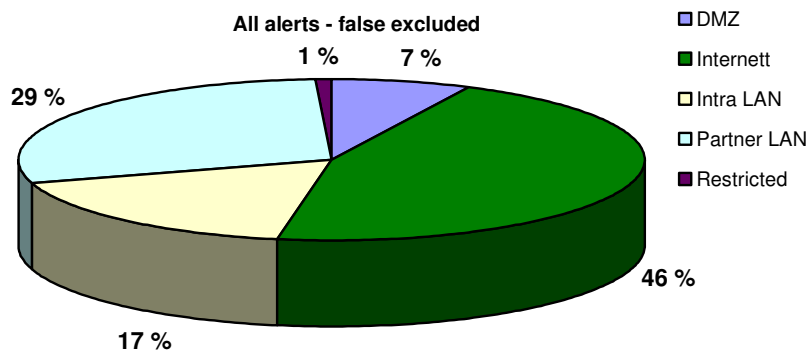
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

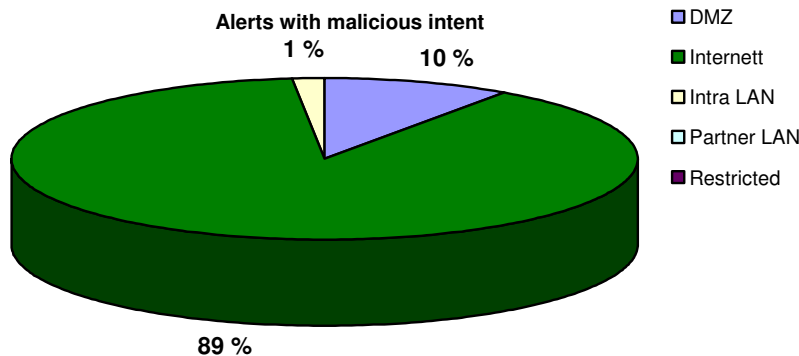
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

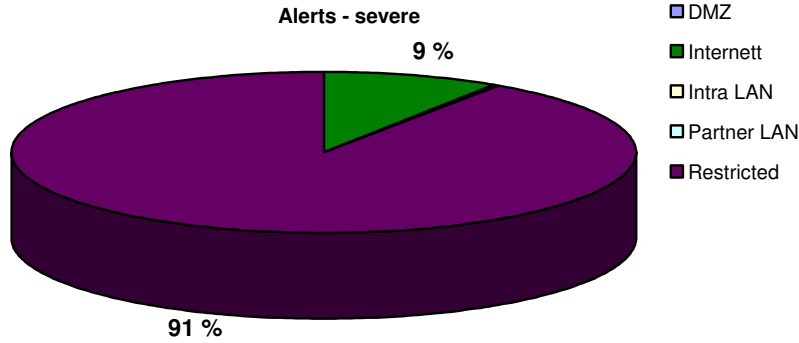
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located inside the network and monitors traffic between clients, servers and other network equipment
- Partner LAN: the measuring point is located in an environment that is used for communication towards external partners. The partner LAN is without Internet access
- Restricted LAN: the measuring point is located in a limited environment with a very well defined traffic pattern and without Internet access



The diagram above shows the distribution for all genuine alerts.



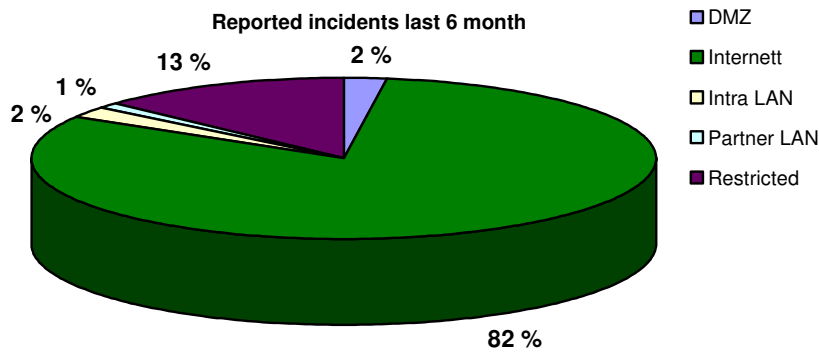
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

REPORTED INCIDENTS

The statistic below shows distribution of incidents reported to customers of Secode the last 6 months.



FOCUS OF THE MONTH – ZERO-DAY ATTACK

An expression that is widely used in IT-security is “zero-day attack” or “0-day attack”.

You would expect that such a well-used expression have a clear definition, but that is sadly not the case. Even in Secode there is some disagreement in what the expression means. This time we will try to describe zero-day attack from the definition mostly used, and we will also try to give some examples on such attacks and shed some light on why zero-day attacks is an important issue for IT-security.

DEFINITION

Mainly there are two definitions for zero-day attack.

1. *A zero-day attack is an attack that exploits a vulnerability for which there is not yet any protection.* [1]
2. *A zero day attack is an attack that exploits a vulnerability on the same day the vulnerability become generally known.* [2]

The first definition contain attacks which get executed on services/vulnerabilities before it become generally known that the vulnerability exist. In other words, an attack performed by a person or a group before it become generally known that the vulnerability exist, is called a zero-day attack. Continued attacks until a patch is released will also be named zero-day attack.

The other definition will only contain attacks which are performed in direct connection with a new vulnerability becoming known.

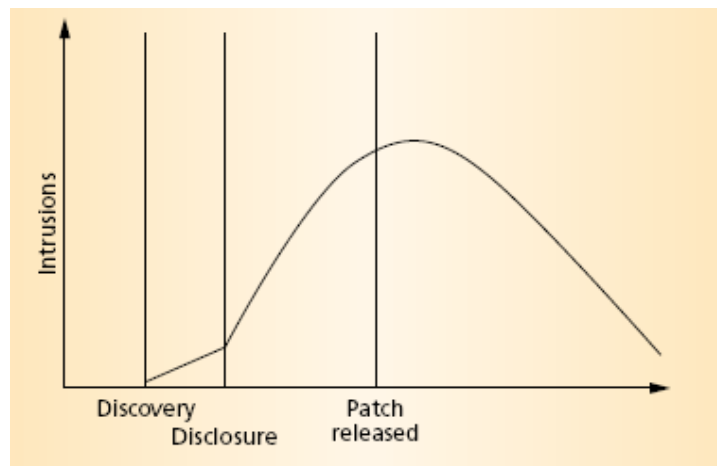


Figure 1 Vulnerability life-cycle [3]

Figure 1 will give an idea of how the different definitions contain vulnerability attacks. While definition two only contains the attacks which happens when vulnerability is disclosed, definition one contains all attacks from discovery of vulnerability until the patch is released.

If we follow definition one, which Secode believes is the most accurate, there are many attacks happening in the period, and many of these will never be discovered since the vulnerability is not generally known.

EXAMPLES

In February this year a Microsoft Word zero-day attack was written about in the media [4]. When a user opened a rigged Word file this could infect the system memory, making it possible for an attacker to gain total control over the computer. As with so many other attacks, this means that the user has to be tricked into opening a file, which then makes it possible for the attacker to enter the system. The day before this exploit was made public; Microsoft released patches for five other zero-day flaws.

This July a zero-day attack towards Internet Explorer and Firefox in combination was made public. This vulnerability may allow the attacker to add commands which then may be run in the vulnerable system. By adding “-chrome” in the run command in Firefox, the attacker could get full possibility to run scripts in the web-browser [5, 6].

This is only a couple of several zero-day attack, and new ones surfaces all the time.

CHALLENGES

The challenge around this is to make the window of time from when vulnerability becomes known until a system is secured as short as possible. The problem is that this mostly depends on the software vendors making a solution available at the shortest amount of time. It is actually the software vendors having control of most of the vulnerability life-cycle. This is shown in figure 2.

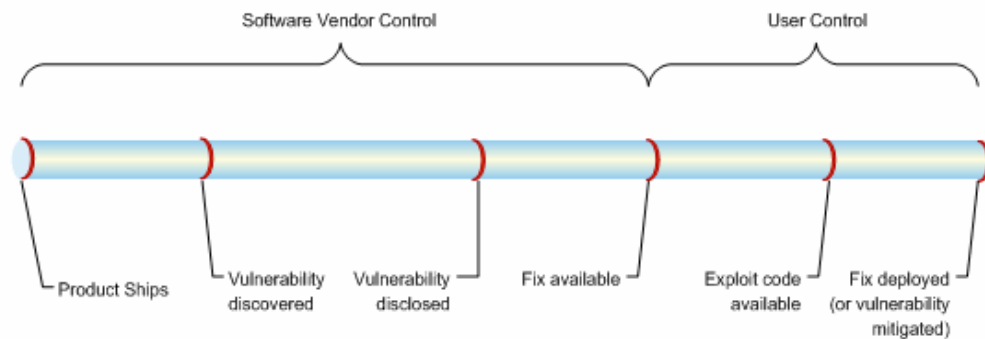


Figure 2 Vulnerability life-cycle and control

The only way for a user to shorten the lifetime of a vulnerability is to make use of the solution as soon as possible. Even though a solution may bring new vulnerabilities, the new vulnerabilities will most likely be less exposed for attack than the old one. This is the reason why it is mostly the best solution to use a fix at the point it is released, even though we will recommend to test the patch in a fairly real environment if it is going to be used on large systems.

SOURCES

- [1] Wikipedia – Zero day
http://en.wikipedia.org/wiki/Zero_day
- [2] SearchSecurity.com Definitions
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554.00.html
- [3] William A. Arbaugh, William L. Fithen, John McHugh, *Windows of Vulnerability: A Case Study Analysis*, Computer, vol. 33, no. 12, s. 52-59, Dec., 2000
- [4] Cnet News.com – Zero-day attack hits Word
http://news.com.com/Zero-day+attack+hits+Word/2100-7349_3-6159824.html
- [5] eWeek.com – Zero-day Hits IE-Firefox combo
<http://www.eweek.com/article2/0,1895,2156543,00.asp>
- [6] ITAvisen.no – Firefox og IE sårbare sammen
<http://www.itavisen.no/php/art.php?id=388886>
- [7] Microsoft Technet: Putting Days-of-Risk to Practical Use
<http://www.microsoft.com/technet/security/secnews/articles/itproviewpoint060904.msp>