

SECURITY THREATS AND TRENDS

NOVEMBER 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 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 level of traffic is now at its lowest registered during 2006 and 2007. This decrease is due to attacks getting more targeted, while reconnaissance attacks are slowly vanishing. It is still VNC services that are mostly exposed, with VNC-1 (port 5901) at the top. It has been a huge decrease in the number of searches towards MS SQL this month.

Among countries of origin we now see that the US is back at the top, after having given this placement to China last month. Norway is still near the top of the list, while Mexico has had the biggest increase since last period.

Spam and worm traffic has surprisingly had an increase this period.

In the focus of the month we take a closer look at the most famous cybercrime group, the Russian Business Network.

TABLE OF CONTENTS

INTRODUCTION	4
THREAT LEVEL	5
RECONNAISSANCE ATTACKS OCTOBER 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 – RUSSIAN BUSINESS NETWORK	11
THE ORGANIZATION – RUSSIAN BUSINESS NETWORK.....	11
ACTIVITIES.....	12
ATTACK TRENDS INFLUENCE	12
LATEST NEWS	13
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 appears when a sensor recognizes network traffic that fits the implemented signatures/filters, and in these cases alerts will be transferred to the Secode SOC (Security Operation Center). All alerts, both false and genuine, are manually handled by analysts at Secode.

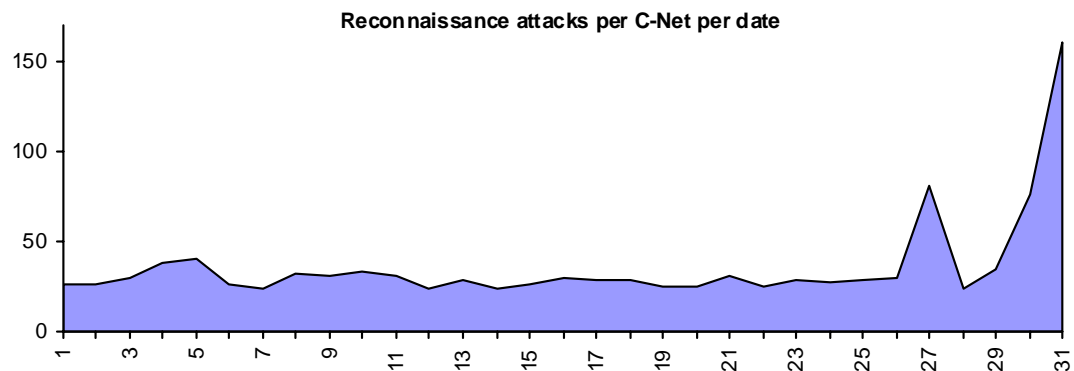
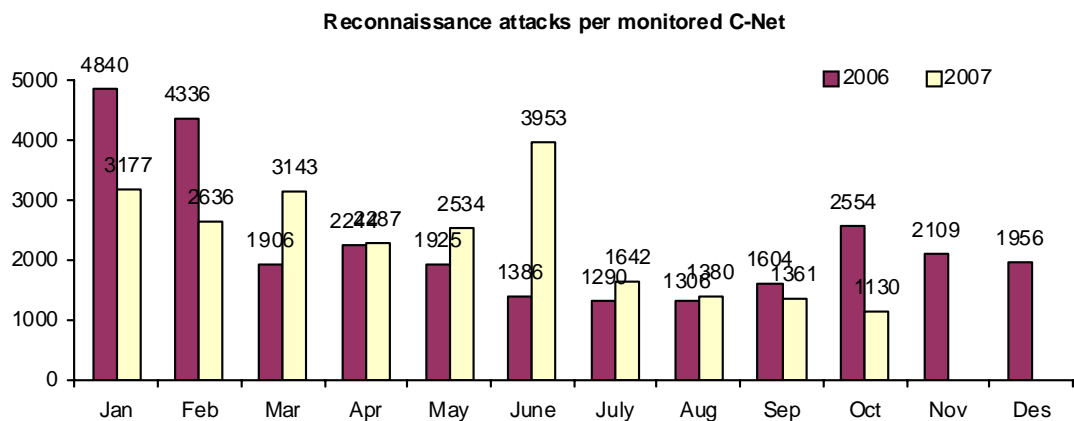
Focus of the Month is an article about relevant topics within IT Security. These might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

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 OCTOBER 2007

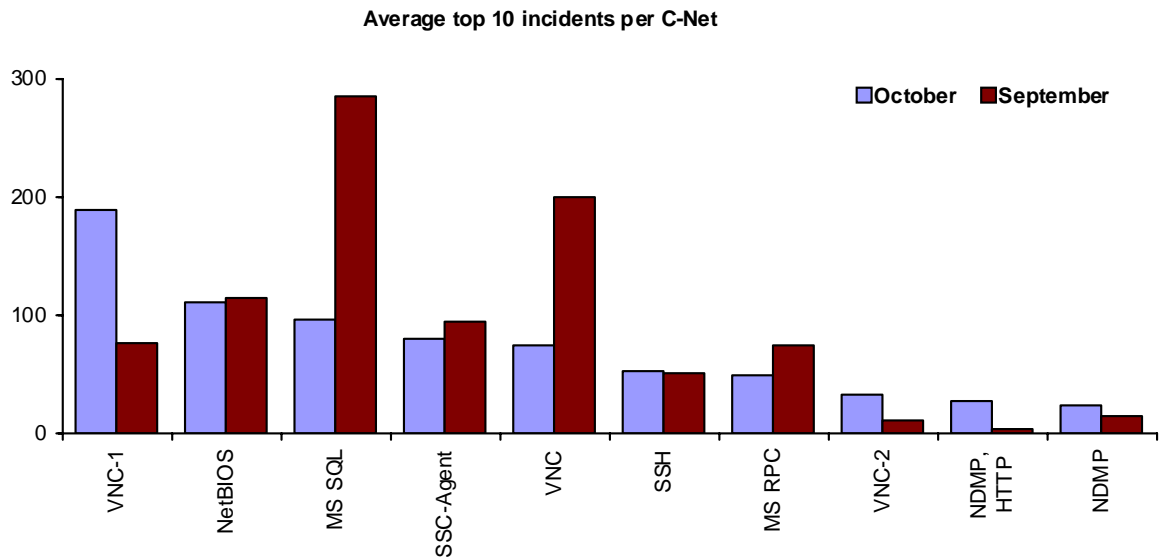
The statistics below gives an overview of the average number of reconnaissance attacks per network under surveillance. However, the activity level may vary from one network area to another. Despite these variations in the total activity level, we (mostly) register the same kind of attacks in different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



There has been a slight decrease in the level of traffic in comparison with last period. We can also see that the level is not at its lowest since January 2006. This decrease is probably caused by the fact that the attack trends have changed a lot during the last year, with more targeted attacks than earlier. It is also likely that increased focus on security both for the private and the enterprise market has caused less machines to be infected with malicious code spreading itself. Most home computers are today secured with both firewall and anti-virus solutions.

TYPE OF RECONNAISSANCE ATTACKS

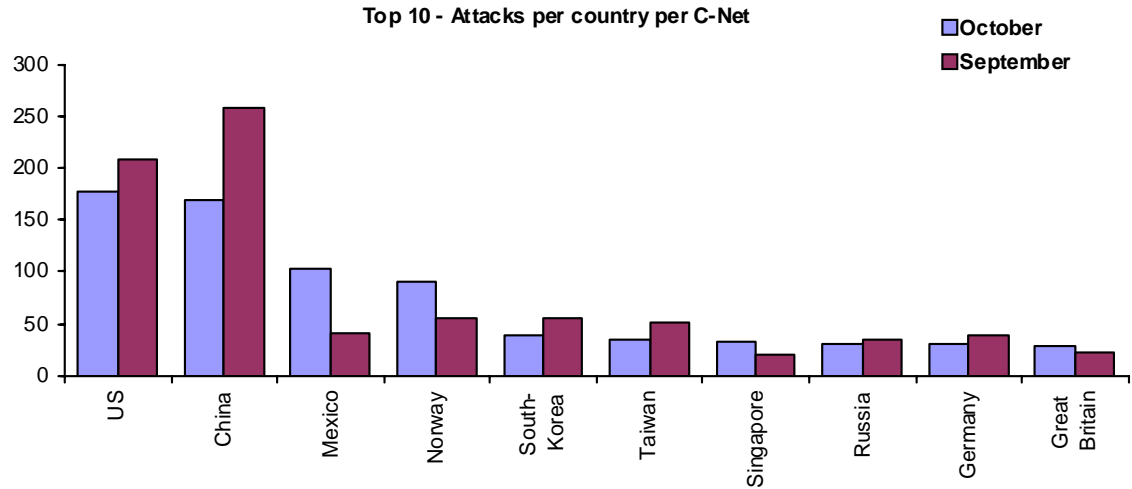
The diagram below contains a summary of the most common reconnaissance attacks during the last two months. The diagram does not separate scans for one single service from combined scans for several services.



The different types of VNC are still targeted, even though we now see that VNC port 5900 have given away its place to VNC-1 port 5901. VNC-1 and VNC-2 have had more focus in web forums lately, and this is probably the reason for these changes. While searches towards NetBIOS are relatively stable, we see a big decrease in searches towards MS SQL this month.

RECONNAISSANCE ATTACKS PR COUNTRY

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



After we saw China passing the US last period, we now see that the US is back at the top. The difference between China and the US is however pretty small. The traffic seen from the US is relatively evenly spread towards all services, while the traffic seen from China is mostly directed towards MS SQL and VNC services.

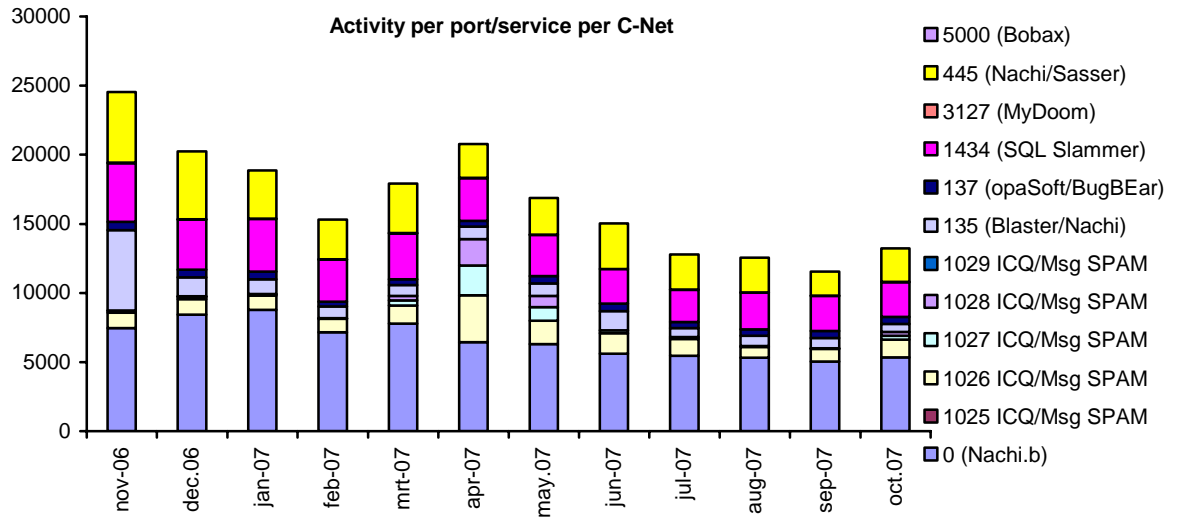
Mexico has had the biggest increase since last period, and most of the traffic from Mexico is directed towards VNC services, VNC-1 in particular.

There has been an increase in the level of traffic from Norway as well this period. The searches from Norway are directed towards most services, but NDMP have been a little bit more targeted this period.

The US is this month followed by China and Mexico.

INTERNET WORMS AND SPAM

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



There has in this period been a slight increase in worm and spam traffic. This we can see especially towards port 445 and port 1026. After a decrease the last periods it was not expected that the level would increase, but the level of traffic is still low in comparison with earlier years.

ALERT STATISTIC

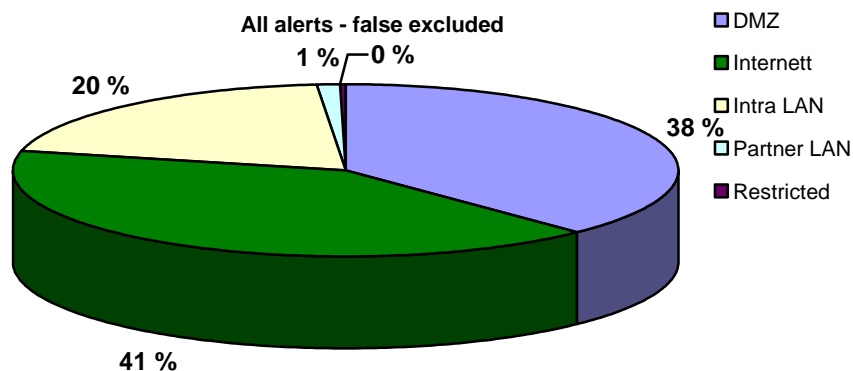
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

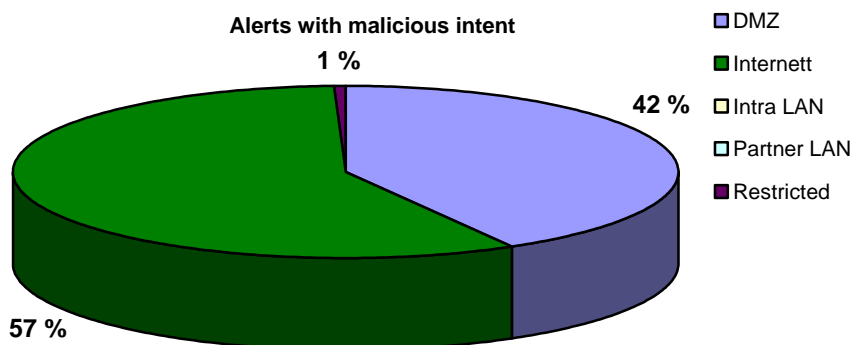
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

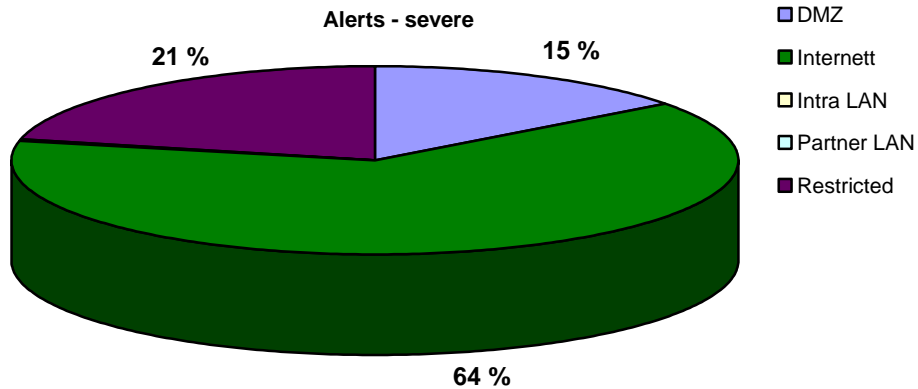
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located 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.



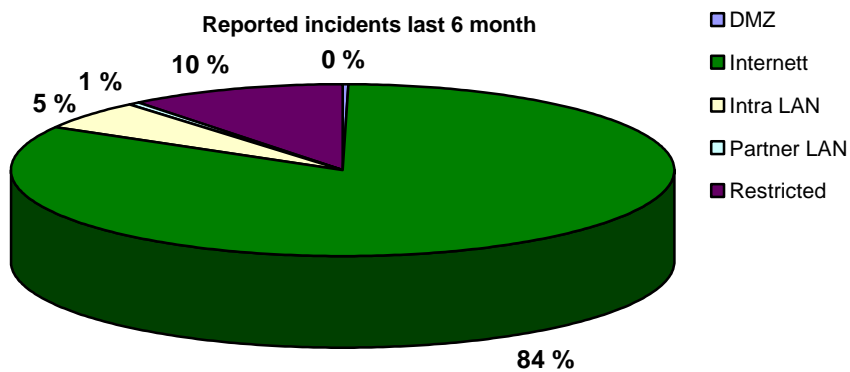
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



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 – RUSSIAN BUSINESS NETWORK

Russian Business Network (RBN) has become today's new Sicilian mob. The Sicilian mob spread to the US in the early 20th century, and it became known for its work in many parts of the world. We see the same approach today by the Russian mob, which Russian Business Network is believed to be a part of. RBN is connected to so many criminal actions on the Internet that it is impossible to cover it all in one article, but I hope this will give some insight in how they operate.

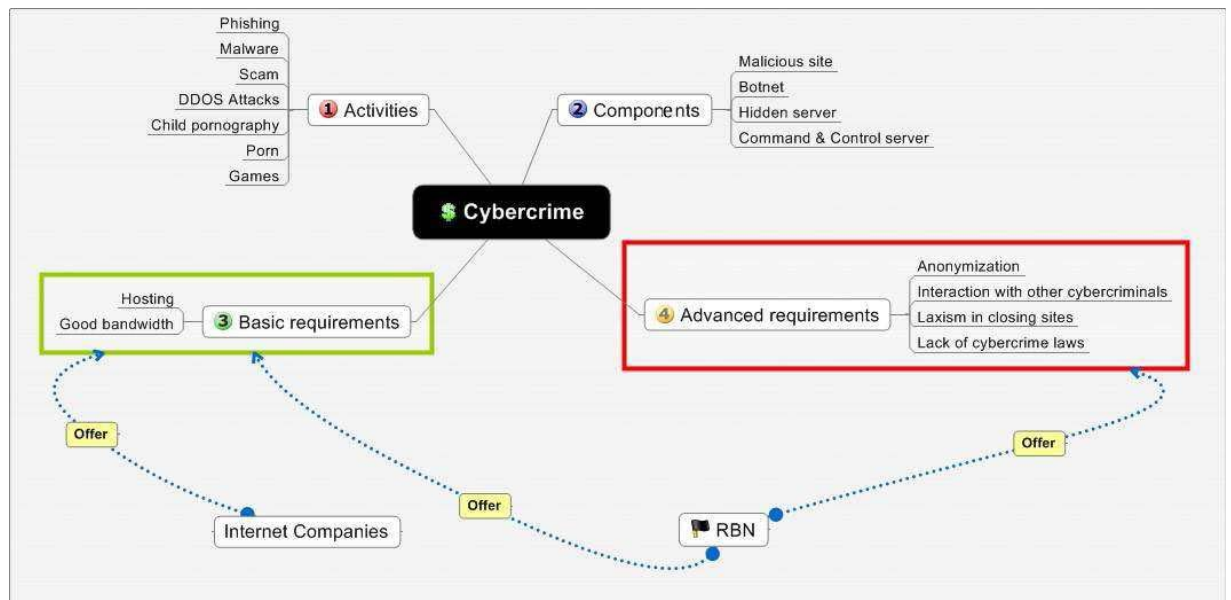
THE ORGANIZATION – RUSSIAN BUSINESS NETWORK

No one is totally aware of how the organization is build. The problem with the Russian Business Network is that they operate under many different names, among these are RBNNet, RBNetwork, Nevcon, iFrame Cash and so on. New connections to the network are continuously discovered.

What we do know with relatively confidence, however, is that the head of the organization is a hacker with the name "Flyman". It is also likely that he is related to a politician in a leading position in the Russian government. In some reports it has become known that RBN is more or less protected by the Russian government, as long as they do not start to attack their own country. The organization with their affiliates is probably divided into four areas of expertise. These are:

- RBN core services
- Hosting
- Telecommunication
- Other services

The figure below gives an overview of which part RBN plays in the cybercrime environment in Russia. The figure is from a report written by an operator at ISC SANS [4].



The main areas of expertise for RBN are hosting, anonymization and interaction with other criminals.

To give an indication of how big an organization RBN really is, we can look at how much they earn per year, which is approximately 150 million US dollars.

ACTIVITIES

There are many activities that Russian Business Network are part of, either directly or indirectly. Phishing, malware, scam, DDoS, child-pornography and spam have all been connected to RBN. We will shortly present some of these areas.

Malware

Russian Business Network have become especially known for selling packages for exploiting known vulnerabilities, but they have had their hand on other things as well.

The most important malware attacks which RBN have been involved with:

- **CoolWebSearch.** CoolWebSearch is installed in the web-browser, and it may then collect information or fetch new types of malware. There is no indication that Russian Business Network has been developers of this, but it is likely that they have hosted servers which have been used for this.
- **MPack.** This is prepared packages which are sold as a finished system. These packages are used for exploiting vulnerabilities in several systems, among others several web-browsers and operating systems. RBN involved persons have probably been developing this system, and there is no doubt that RBN have had several malicious servers in connection with this. In September this year it was estimated that around 500 000 machines have been infected through 3.1 million attacks. It is expected that several more have been infected since this estimate was done.
- **Torpig/Sinowal.** This is a group of Trojans which are mainly used in connection with online banking frauds, and is sold by RBN. Several Nordic banking services have been targeted by this as well. The most known case is an attack towards Nordea Sweden, which was executed by a Trojan like this in late 2006 early 2007.

Phishing

There are actually no reports that RBN is hosting any phishing sites. However, there is no doubt that RBN is indirectly connected to phishing, since many of their Trojans for online banking frauds are spread through phishing sites.

Spam

Spamhaus have registered RBN in their ROKSO (Register Of Known Spam Operations) database. Here they are listed as "Among the world's worst spammer, child-pornography, malware, phishing and cybercrime hosting networks."

Shortly, Russian Business Network has become known for being connected to most of the malicious acts on the Internet. RBN is described as "the baddest of the bad".

ATTACK TRENDS INFLUENCE

Lately we have seen that the attack trends are directed more and more away from the reconnaissance attacks, and they are directed towards specific targets. In many ways you can say that Russian Business Network have had relatively big influence on these trends. We can see this through many attacks of the Mpack type, which is adapted to the needs presented, in other words which information they want to retrieve. Online banking Trojans are also directed towards one goal, the online banking services. The online banking services in question must be coded in to the Trojan, and they are in other words customized after the intended victim.

As long as RBN or other similar organizations exists, we will continue to see some changes in the attack trends. We will see more attacks that are goal-oriented, but still is built on nearly finished solutions. In this way hackers, and other cyber-criminals, can achieve as much as possible without the traffic hitting more than necessary.

LATEST NEWS

The latest news about Russian Business Network is that it seems like they are relocating. After increased focus and pressure towards RBN and some changes in the routing possibilities in Europe, they have more or less been forced to find new areas to locate their servers. At this moment huge parts of RBN are vanishing from the Internet, but they are believed to resurface soon, probably located in China.

There is however a big part of RBN still working as usual, with some new locations, and the activity from RBN is still large. The last known attack related to RBN was reported November 19th. This attack was an attack where iFrame vulnerabilities were exploited, which is sold as a part of the MPack solutions.

There is no reason for believing we will see less of RBN in the future. There is actually a chance that they will resurface bigger and stronger than ever, something that most IT-security experts see as a big challenge.

SOURCES

- [1] Wikipedia – Russian Business Network
http://en.wikipedia.org/wiki/Russian_Business_Network
- [2] Wikipedia – CoolWebSearch
<http://en.wikipedia.org/wiki/CoolWebSearch>
- [3] Blogspot – Russian Business Network
<http://rbnexploit.blogspot.com/>
- [4] David Bizeul – Russian Business Network Study
http://www.bizeul.org/files/RBN_study.pdf
- [5] The Diplomat – World Wide War 3.0
<http://www.the-diplomat.com/article.aspx?aeid=3301>
- [6] Softpedia – Russian Child-Porn Hosters Guilty for Band of India Hack
<http://news.softpedia.com/news/Russian-Child-Porn-Hosters-Guilty-For-Band-of-India-Hack-64524.shtml>
- [7] The Age – From Russia with malice
<http://www.theage.com.au/news/business/from-russia-with-malice-criminals-trawl-the-world/2007/07/23/1185043032049.html?page=fullpage#contentSwap1>
- [8] iDefense – Global Threat Research Report: Russia
<http://www.pmi.it/file/whitepaper/000185.pdf>
- [9] Washington Post – Russian Business Network: Down, But Not Out
http://blog.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html?nav=rss_blog