

ATTACKS TO INTERNET LINKS

JULY/2004

Silent attacks

We present in this paper an analysis of the volume of non authorized attempts to access of a set of corporate networks managed by i.web.

None of the networks studied had its security compromised, however, the quantity and the characteristics of the attacks are significantly high to justify a special attention to this subject.

The primary goal of this report is to provide a quantitative measure of the daily attacks involving common corporate networks, detailing the need for infrastructure investment to raise the level of security for all types of business.

Observations and acknowledges

In order to respect the privacy of our customers, we omitted all data that could identify them or put their business at risk. i.web customers under the 24x7 monitoring contract will receive a detailed report with the analysis of their network infrastructure, including a comparative between their networks and the set of networks being studied. The detailed reports will be ready by the end of July 2004.

We specially thank our customers who allowed us the use of their data to develop this report. We hope the study presented here help them make their networks more secure.

Methodology

The analysis is based on data collected from April to June of 2004 and it is firstly separated by the broadband type and secondly by date and time of occurrence, protocol type, access port and content. This paper shows only an excerpt of the report, organized by link type, i.e., the first level of separation described in the last paragraph, leaving the remain levels to each customer detailed report.

Link type	Share
Frame relay	21.73%
ADSL	63.68%
Radio	14.59%

Table 1 – Participation of each link type

Results

Radio links seem to be the main target to attacks, concentrating almost 70% of the packets, which is about 4 times as many packets as ADSL links (Charts 1 and 2). ADSL links, the most popular in small and medium size companies, show an anomalous behavior: the number of attacks varies significantly from 30.000 to 230.000 per month depending on the company (Chart 3). Frame relay links appear to be the less vulnerable type, maybe because the other types are know to be more insecure.

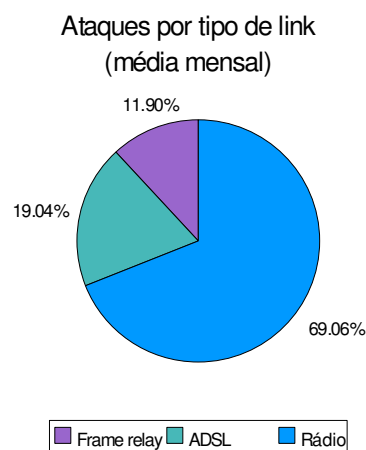


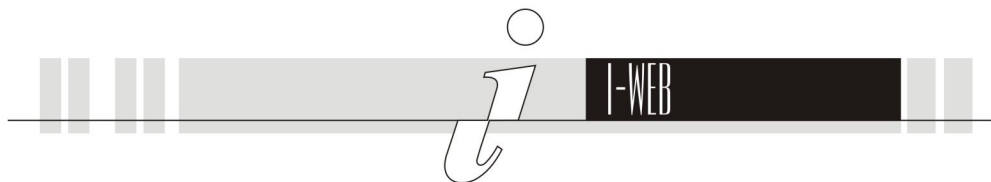
Chart 1 – Attacks by link type

Despite the majority of the attacks were simple and easy to defer, the volume was significantly high, reaching alarming average values, as shown in Table 2.

Average by link type	Attacks / hour	Attacks / minute
Frame relay	93.9	1.6
ADSL	150.3	2.5
Radio	545.2	9.1

Table 2 – Attacks by link type

Table above shows that there is one attack each 24 seconds in ADSL links and one attack at each 6.6 seconds in radio links. Even considering none of those attacks had succeeded, the high volume of "invalid packets" generates enough traffic to slow



ATTACKS TO INTERNET LINKS

JULY/2004

down the network, and reducing the performance of systems, websites, VPNs, and so on.

attacks against frame relay links usually are the most sophisticated ones, even though in small number.

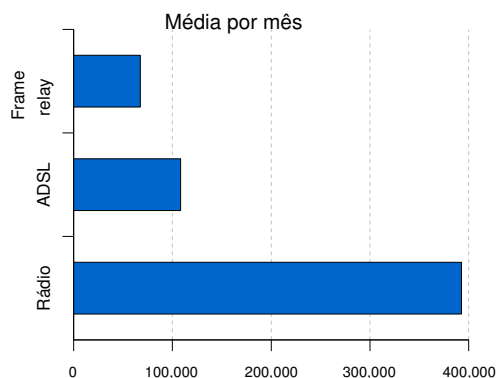


Chart 2 – Monthly average

There were attacks against Windows, Unix and Netware platforms. However, Windows exploits, which affect IIS web servers, Exchange and File servers, were far more explored.

Independently of which platform has been attacked, in most cases the attacks had focused platform known vulnerabilities. Unpatched systems would be affected by most of the attacks.

A significant share of packets originated outside Brazil, mainly in Asia, Eastern Europe and North America.

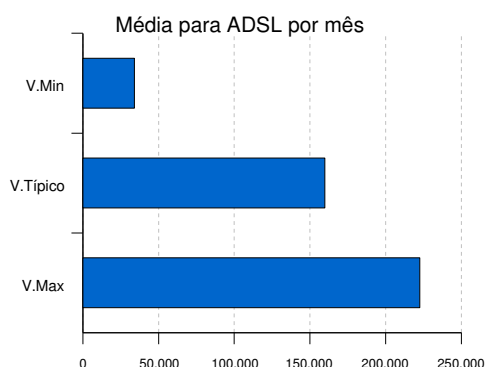


Chart 3 – Attacks against ADSL links

The analysis has shown that most of the attacks against ADSL links, aim to gain access to vulnerable machines in order to use them as open relays (and subsequently as a SPAM sender). On the other hand, attacks against radio links seem to gather unencrypted data from those networks. Finally,

Security

Although most of the attacks do not aim a company, but an IP address, in other words, they are random attacks with no knowledge of the actual IP owner and therefore, without any interest in one particular company, several companies suffered attacks from their competitors.

Counterattack

The majority of the networks observed during the that period were protected by firewalls and intrusion detection systems (IDS), what made easier the attack detection and reaction, preventing them from succeed. The 24x7 monitoring proved to be a valuable tool, given that the attacks occurred along 24 hours of day, keeping the same pace during the weekends.

Conclusion

Although most users imagine that a firewall is the ultimate protection for their networks, this study shows the necessity of a more complex infrastructure and a constant vigilance and the use of appropriate tools to protect the network, acting and reacting when necessary.