The CyberAbuse Project

FIRST 2002

Philippe Bourcier

1. Introduction

Because of the strong evolution of Internet and because there will never be enough done for its safety, CyberAbuse has widen its scope by developing some new exciting projects during the last few months.

This paper presents the new CyberAbuse projects but also statistics and results from our active projects.

2. Results and statistics

2.1. Smurf amplifiers statistics

Abuse-DoS is the CyberAbuse project focused on smurf amplifiers. It is based on the work of volunteers who mail administrators of networks listed in our database. The database has been made from the networks listed on the SAR (Smurf Amplifier Registry) and netscan.org databases. Before each mail sent a test of the possibly misconfigured router is done.

Note that SAR is not working anymore, due to pressures from the hosting ISP. Indeed, it is clear that such websites, providing lists of smurf amplifiers to everyone are more used by script kiddies than by administrators.

The Abuse-DoS project volunteers worked on what was called the “first pass” from June 2000 to May 2001. Then the system was rebuilt using a new tool, abuseEmail that finds the NOC contact e-mail address automatically by parsing the whois databases.

In September 2001, before launching “pass two”, we decided to check for existing smurf amplifiers on our whole database. The result of this was the removal of 17000 smurf amplifiers from our database, which means the administrators of those 17000 networks had received a mail from us and because of it or not, had fixed their network. But often, administrators fix more than one network at the same time, which has been verified by the growing number of networks found fixed along the first pass.

The volunteers are now working with the “pass two” system since September. We expect that in the end of this pass, there will only be 50000 active smurf amplifiers left.

Some companies and organizations with a huge amount of misconfigured routers made a big effort to solve the issue as shown in the table below. The number of smurf amplifiers in Japan is decreasing even at OCN (9% of the smurf amplifiers in database) but in the same time new networks appears from Korea in particular. It is interesting to compare this table with the misconfigured proxy servers one (see 2.2).

Top 20	May 2001 (pass 1 ended)		November 2001 (pass 2 in progress)	
	Company	**Country**	**Company**	**Country**
1	NTT (OCN)	JP	NTT (OCN)	JP
2	Verio	US	Southwestern Bell	US
3	Southwestern Bell	US	Dion	JP
4	Japan Telecom (ODN)	JP	Verio	US
5	Sprint	US	Bell	CA
6	Dion	JP	Sprint	US
7	AT&T	US	PSI	US
8	Government of British Columbia	CA	UUnet	UK
9	UUnet	UK & DE	Telstra	AU
10	Ministry of Education	TW	Dreamline	KR
11	XO Communications	US	ChungHwa Telecom (HiNet)	CN
12	BellSouth	US	MCI WorldCom	US
13	Cable & Wireless	US	Cable & Wireless	US
14	ChungHwa Telecom (HiNet)	CN	Ministry of Education	TW
15	Interlink	JP	Japan Teelecom (ODN)	JP
16	Qwest	US	AT&T	US
17	Digital United	TW	DACOM	KR
18	Chinanet	CN	Chinanet	CN
19	MTT	US	Global Crossing	US
20	Telstra	AU	BellSouth	US

Comparative table of the numbers of companies we contacted about smurf amplifiers before May 2001 and between May 2001 and November 2001 sorted by number of e-mails sent.

2.2. Misconfigured Proxy servers statistics

Abuse-Proxy has been in preparation since February 2001 and has finally been launched at the end of October 2001. The project is focused on fixing misconfigured proxy servers. The projects database is filled with the UnderNet IRC network proxy scanner logs, which are sent to us daily. This IRC proxy scanner is different from the others since it does not only check for a misconfigured socks server, but also checks for misconfigured Wingate, Socks 4/5, Squid proxy and HTTP proxy servers.

Indeed, since January 2001, kiddies and affiliates seem to have discovered that they could easily use misconfigured HTTP and Squid proxies to connect multiple clients and abuse the UnderNet IRC network.

By that time, a vulnerability was found in some corporate proxy/cache systems (CacheFlows), which were allowing the whole Internet to connect through them.

As the UnderNet proxyscanner is GPL software, we expect many other major IRC networks to use it. Included in the software package are explanations of how to easily send the daily proxy scanner logs to our server through a SSL tunnel.

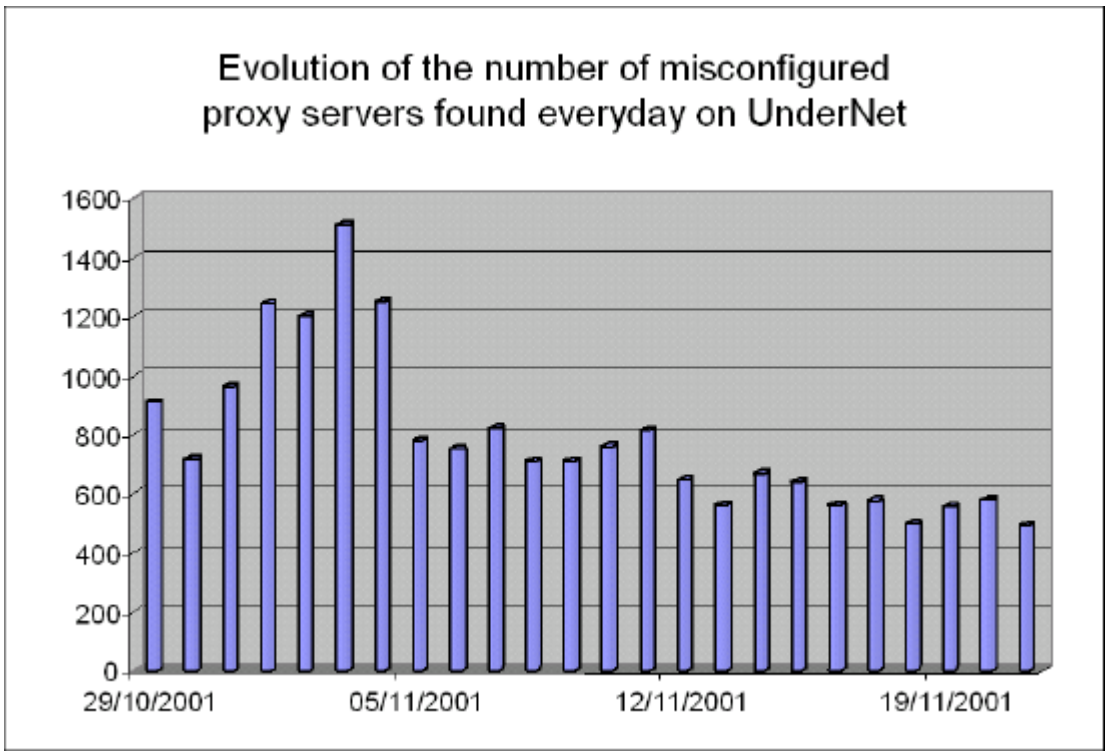
Type of proxy	Wingate (port 23)	Socks 4 (port 1080)	Socks 5 (port 1080)	Squid / Winroute (port 3128)	HTTP proxy (port 8080)
Percentage	5.2 %	60.8 %	6.0 %	21.6 %	7.4 %

Percentages of types of misconfigured proxy servers detected on the UnderNet IRC network.

You can notice in the above table that the Squid and HTTP proxies represent 29% of the misconfigured proxy servers that try to connect to the UnderNet network. We wondered why there were so many squid proxy compared to the other types of HTTP proxies and we found that the connection sharing and proxy software "Winroute for Windows" also uses port 3128 by default for its proxy server; and that by default if the user doesn't set any ACLs, it simply allows everybody from the Internet to use that proxy (from their website: "WinRoute Pro is a robust network firewall…"). The number of misconfigured Socks server is very impressive, more than 65%, a lot of those are Socks 4. Those socks servers, in opposition to the common belief are mostly running on Windows systems (MS proxy, WinProxy, SyGate…).

The Abuse-Proxy project is not old enough to have clear statistics about its results. Anyway, there are hints about its success in the numerous mails received and in the below graph, which presents the number of proxy servers found daily on the UnderNet network. As you can see on the graph, the number of misconfigured proxy servers found is decreasing. There are three reasons for this:

- A user is running an open proxy and can't connect anymore to UnderNet anymore, so they check their configuration and fix their proxy server.
- The people who were abusing open proxies has realised they couldn't anymore.
- The users, customers or administrators responsible for the open proxy have received the Abuse-Proxy e-mails and fixed the misconfiguration.



Below is a table which presents the Top 10 ISPs we have contacted about open proxies found on their networks. Three Americans ISP are in both the smurf amplifiers Top 20 and the open proxies Top 10.

Top 10	Company (country)
1	EXcite@home (USA)
2	Bell (Canada)
3	Road Runner (USA)
4	Vidéotron (Canada)
5	Chello/UPC (Netherland)
6	Southwestern Bell (USA)
7	Telefonica São Paulo (Brazil)
8	Wanadoo (France)
9	Ati.tn (Tunisia)
10	BellSouth (USA)

Every week, an automatic system mails the administrators of all the misconfigured proxy servers found on UnderNet during the past week. The automatic system is based on the CyberAbuse whois server (see 3.1). This allows us to include in a single mail to an ISP all the IPs found during the week. Approximately 2000 e-mails are sent every week, with an average of 4 IPs per message.

3. New projects

3.1. The CyberAbuse whois server

The CyberAbuse whois server finds the abuse contact e-mail for a specific IP in the different whois databases available. It finds the appropriate e-mail more than 97% of the time and operates at an average speed of one IP per second.

While this tool was designed to help the CyberAbuse projects, we also wanted it to be more widely used and useful, hence the creation of the whois.cyberabuse.org server and the http://www.cyberabuse.org/whois/ website. This public whois server is made to help home users and administrators to easily get the abuse-contact for an IP and is also made to improve the work of incident response teams. An open source version of the tool for unix like systems should be released later this year.

Also one of the main problems CyberAbuse had with any previous system was the fact that administrators couldn't easily modify the e-mail used to contact them, this is now solved. In every e-mail we send now we include the whois website URL, so administrators can easily modify the abuse-contact e-mail used for their networks.

An application of the tool, such as mailing ISPs with misconfigured proxy servers on their networks, for 8000 proxy servers takes about 2 hours, this work would normally take more than five days with two people working full-time (doing 800 whois queries a daily).

3.2. The CERT-IRC project

CyberAbuse has always and will always be strongly linked to the IRC world and the IRC networks. While all the large IRC networks have more or less organized an abuse team to reply to user's complaints, a few have set up teams which are focused on contacting administrators about incidents happening on IRC. Those teams do not communicate between each other and most of the time, after a few months of labour, the lack of means and appropriate tools causes a loss of interest and motivation for the volunteers.

CERT-IRC is an online incidents and abuse management system focused on:

- Providing an efficient incident management system to network officials
- Communication between IRC networks
- Communication with other CERTs and IRTs
- Providing a system for IRC users to report hacked hosts, spam, virii…

This project should be released at the end of November 2001.

3.3. CrimeWatch forensics challenge

CrimeWatch is a mailing list founded in 1994 in order to provide law enforcement agencies and system administrators with shared information as pertaining to Internet related criminal activity. CrimeWatch is limited to law enforcement and security professionals.

During the last few months, CrimeWatch moderator with the technical help of two CyberAbuse developers organized a forensics challenge, which should be launched in January 2002. The first CrimeWatch challenge is entitled “digging clues out of IRC logs”. Our goal is to provide methods and tools to help law enforcement, forensics experts and security professionals to work with such materials. Real-time chat systems are very different from fax, phones, e-mails and other mediums. Under a simple chat system there is a powerful tool, which can be used for much more than just “chatting”. Script kiddies and other abusers have understood this and have developed tools, trojans and virii based on IRC communication.

3.4. Web proxyscanner

The CyberAbuse website now provides a proxy scanner which can only scan the IP browsing the website or the one under a proxy. The URL of this scanner is included in all the e-mails we send to administrators so they can provide their users with a tool to verify that the fixed their misconfiguration.

4. Projects under development

4.1. RootkID

This project was presented during the last FIRST conference. RootkID will be the first database with checksums of rootkits, trojans, sniffers and other tools that could be used in a system compromise. This database should help administrators to find the most common files left by an intruder but it should also help them to verify if their system hasn’t been compromised.

4.2. Abuse-Proxy DNSBL

The first usage for this DNSBL will be for spam filtering purpose, since spammers use many open proxy servers.

The second use is more specific to misconfigured proxy servers. An Apache web server module called mod_proxykiller will use the DNSBL to deny access to any proxy listed who try to access a website running on that web server. This should help many free hosting providers in their fight against people who register account to host illegal content. But this should also help websites with pages under restricted access, which are often bruteforced. This module is currently being developed.

4.3. CyberAbuse Whois

A future feature of the CyberAbuse whois is to add information about the CERT or IRT to which an incident or abuse complaint could be forwarded while contacting the administrator of a network.

A version of the CyberAbuse whois for Windows with a graphic user interface will be developed for the vast community of home users or administrators who use this OS.

A plugin for the well-known and widely used Snort IDS could be developed. This plugin would automatically contact the administrator of the network on which a compromised system launching serious attacks would be hosted. This could also be a manual feature included in the ACID frontend for browsing Snort logs. The mail template would include the packet stream received with the necessary timestamps.

5. Conclusion

2001 has been a very busy year for abusers but also for the people fighting them. Our actions have been proven to work and we are now taken more seriously than ever. There has never been such a good collaboration between our organization and other parties, may they be ISPs, administrators or IRTs.

CyberAbuse will become an official organization in France during 2002. Our new projects needs resources, which demands funds. We hope those who make Internet work and its citizens will help us in our effort to fight back abusers by putting their toys out of action.

6. Thanks to …

All the volunteers, who did a great work again this year.
This page is dedicated to them: http://www.cyberabuse.org/?page=the_team

Abuse-DoS project leader: Jack Carreiro
Abuse-Proxy project leader: Lynn Stodola
UnderNet Proxyscanner by Stéphane Thiell: http://pxys.sourceforge.net/
Web Proxyscanner by Stéphane Thiell: http://www.cyberabuse.org/?page=proxyscan

Companies hosting and providing servers for CyberAbuse:

- OVH.FR: www.cyberabuse.org (web server + Abuse-DoS)
  gizmo.cyberabuse.org (Abuse-Proxy, CERT-IRC)
- BIT.NL: whois.cyberabuse.org (whois server)
- Peter van Dijk (NL) : monster.cyberabuse.org (web proxyscanner)