Michael Poor
SANS Security Essentials
GSEC Practical Assignment
Version 1.2e

Title: The Brazilian Connection: Brazilian Defacement Groups Stake their Claim

On June 22, 2001, Prime Suspectz, a Brazilian hacker group, defaced four Microsoft sites in less than one hour[1]. According to one of the pages they defaced, three of the sites were defaced in just half an hour!

Brazil is a country of impressive statistics. A land of contrasts, Brazil is the 5th largest country, and one of the largest economies in the world[2]. Despite its wealth of natural resources and large labor pool, Brazil is a country with extremely unequal distribution of wealth.

Brazil also accounts for an enormous amount of Internet attacks. Analyzing the top 50 website defacement groups from Safemode.org[3], I discovered that 30% are Brazilian.

The web is the front-line for future warfare. According to Lawrence Gershwin, the CIA's top advisor for science and technology, "we anticipate more substantial cyber threats in the future as a more technically competent generation enters the terrorist ranks"[4]. He points to hackers from China and Russia, as being our biggest enemies. Taking this a step further, we can see that the future of warfare might be in the hands of individuals, as opposed to the giant and hyper-funded armies of the world. The U.S. and other major players have their information warfare divisions, but small groups with private agendas, have minimal overhead and can impart a large impact on economies worldwide.

While the United States is preoccupied with China and Russia as its greatest cyber-enemies, countries like Brazil go almost unnoticed. Last year, the U.S. was forced to take notice when a Brazilian group known as Inferno.BR broke into NASA and NATO. Inferno.BR was a group of Brazilian hacktivists, whose primary goals was to voice its disapproval of the Brazilian government, as well as point out objectionable international policies that affected Brazil and other developing nations. Two members of

Inferno.BR were caught: JxLxMx, 21 years old, and JamiezJamiez who was 22. Neither had a previous criminal record[5].

Through the course of this paper, I will profile three current Brazilian hacker groups, BHS [Brazilian Hacker Sabotage], Prime Suspectz, and Perfect.BR. These three groups account for over 1346 defacements since October of 2000! These attacks, by these three groups, account for 6.63% of all defacements tracked by alldas.de[6].

BHS [Brazilian Hacker Sabotage]

*[7]

Quick-view
Members: Jshalom ; Astek; Tuk
Contact:jshalom@brasnet.org; tuk@brasnet.org; astek-bhs@hushmail.com
IRC:#BHS on irc.brasnet.org
Sites Defaced: 627[8]
Safemode.org's Rank: 3rd[9]

BHS is comprised of three people, Jshalom, Astek, and Tuk. Another member, dAnGeRmOuSe appears to have left the group or changed his nic [nickname]. As per safemode.org's records, BHS is the 4th most prolific hacker group on the net, one above the infamous PoisonB0x[10].

BHS has defaced 604 sites, according to the Alldas.de defacement archive [up to July 6, 2001]. At least 443 of these servers were running Microsoft Windows operating systems. From this we can presume that this group specializes in Windows hacking, although we must note that they did break into 118 Linux servers as well[11].

BHS defaced over 30 sites between July 1 and July 4th.[12] Many of these pages are still live with the defacements showing. BHS, in a recent statement on a defaced Malaysian page, taunts that .my [The country Top Level Domain for Malaysia[13]] was missing from their collection of Top Level Domains[14].

Competition is common among the black hat community. Hackers compete for the overall quantity of hacks, quality and difficulty of the hacks, fame of the hacked site, and general publicity or infamy.

BHS is a high-profile hacker group, given the sheer number of sites that they manage to break into and deface. This group is very active in attacking .com domains, which account for 207 of the 583 sites studied. This is a large number, when comparing this statistic to: 53 .b [Brazil's TLD] domains, 1 .gov [U.S. Government TLD], 10 .cn [China's TLD], and 23 .tw [Taiwan's TLD] domains. There were no registered attacks by BHS to .mil [U.S. Military TLD] domains[15].

I wrote to the members of BHS requesting an interview, but they declined.

Prime Suspectz

[16]

Quick-view
Members: x-s4nd3r ; k4m1k4z3 ; 4n1c1l4t0r
Contact: psuspectz@mail.com
IRC: n/a
Sites Defaced: 495[17]
Safemode.org's Rank: 22nd[18]

Prime Suspectz is comprised of three individuals: x-s4nd3r [pronounced X-Sander}, k4m1k4z3 [kamikaze], and 4n1c1l4t0r [anicilator]. Their average age is 18.

Prime Suspectz sets itself apart from the crowd not only by overall numbers of sites attacked, but in the quality of the hacks perpetrated.

As previously mentioned, on June 22, Prime Suspectz hacked 4 of Microsoft's sites in less than an hour. The four sites were: webcfeedback.msn.com, arulk.rte.microsoft.com, feeds.mobile.msn.com, and redsand.rte.microsoft.com[19].

On the first site, webcfeedback.msn.com, Prime Suspectz left the following message: "Prime Suspectz is back micro$oft.. + 1 for the collection.. when your security will go to improve? never hehehe! kisses adm gay!"[20]

On the second site, arulk.rte.microsoft.com, they left: "Prime Suspectz onwed microsoft one more time!! mais uma pro saco..."[21] [The last part says: one more for the sack].

The third Microsoft site they defaced boasts: "Prime Suspectz again!.. one, two, three, in only 30 minutes, As we can see, this server IIS is very good!! Micro$oft, where i find secure products made by you? WHERE?...i like to say hi to Crime Boys, IZ Corp, Supre Entity, pr0phet, n0id and all WoH!"[22].

Finally the fourth Microsoft site simply states: "Prime Suspectz again!"[23].

These recent attacks are an example of Prime Suspectz searching out a target and then defacing it. There were no important political messages stated, just the implied message that the servers were not secure, and that Prime Suspectz could hack them at will.

Prime Suspectz is definitely a group to keep track of, as they consistently hack high profile domains, and attack multiple operating systems. Their cadre of hacked operating systems runs the gamut, excluding perhaps only Apple [for the time being]. Prime Suspectz have hacked 1 .mil [U.S. Military TLD], 16 .gov [U.S. Government TLD], as well as many Taiwanese, Chinese, Japanese Top Level Domains[24].

Following is an interview I conducted with Prime Suspectz, on June 30, 2001. This interview is translated from Portuguese.

Interview with Prime Suspectz

Q. Why do you think that there are so many defacements coming out of Brazil? Social Conditions? Politics?

A. Here in Brazil we have many groups that support the freedom of information, and it is very easy to find material and knowledge to start invading sites.

Q. What is the reason that your group defaces sites? What do you expect to gain from this?

A. In the beginning, it was for social and political motives but now it is just for fun!

Q. What is your favorite Operating System, for home, for hacking, and for work?

A. The O.S. that I love to hack the most is Solaris, but our strength has always been Windows hacking. At home I use FreeBSD and Linux.

Q. For your defacements, you seem to seek out various Operating Systems? Do you like the challenge? Or is there another reason?

A. We like to hack different O.S.'s for one reason… KNOWLEDGE. Always invading the same OS with the same bug is boring. That is why we go after different Operating Systems.

Q. Do you find many low lying (easy to exploit) vulnerabilities? (i.e. Unicode, directory transversal, and BIND vulnerabilities)

A. These days, that is what we find the most. ☺

Q. What is the vulnerability that you find the most?

A. In windows we exploit the cgi decode bug and printer bugs a lot, and in other OS's, well, that's a secret.

Q. How do you target sites to deface?

A. These days we hit Microsoft a lot, we love invading them ;)

Q. If you had to choose just one hacking tool, what would it be?

A. I don't know man, I had never thought about that.

Q. What is your best advice to system administrators?

A. Visit security sites every day, and always keep up to date wit the newest vulnerabilities.

Q. Do you work with other international groups? Did you participate in project China or something similar?

A. No, we work alone.

Q. What is the average age of your members?

A. 18

End of the Interview with Prime Suspectz.

Perfect.br

[25]

Quick-view
Members: ScorpionKTX ; ph4r0x ; USDL
Contact:perfectbr@inferno.com
IRC:
Sites Defaced:224[26]
Safemode.org's Rank:9th[27]

Perfect.br is a Brazilian defacer group comprised of three individuals: ScorpionKTX, ph4r0x, and USDL. Their ages range from 15-18 years old. They are ranked 11th on Safemode.org's Top 50 defacers records[28].

Perfect.br routinely leaves behind a message: "Oportunity favors a prepared mind"[29]. This echoes the message from recent interviews that I have conducted, in which hackers say that the most important thing for system administrators to do, is to keep up to date with the latest vulnerabilities and security news.

Looking through the alldas.de defacement archive, we see two interesting trends related to Perfect.br. In the last thirty days, Perfect.br has attacked 9 banking institutions, and multiple educational domains, including subdomains at Harvard and Princeton[30].

Perfect.br is a force to be reckoned with in the commercial world, although they have not defaced any .gov or .mil sites. It is important to note that even though they have not attacked U.S. Government sites, they have recently hacked a British Virgin Islands Government site (www.bvigovernment.org), and have attacked Brazilian government sites in the past (i.e. www.trt17.gov.br)[31].

Perfect.br appears to be a Windows defacement group, as 177 of the 182 sites studied were running a Microsoft Windows Operating System. It is interesting to note that in my interview with Perfect.br, they mention that the main reason that they have attacked windows boxes is that many well-known sites are running Windows. Perfect.br also points out that most well known sites that are running *nix flavors are pretty well locked down.

Following is an interview I conducted with Perfect.br on June 19, 2001. The interview is translated from Portuguese.

Interview with Perfect.br

Q. Why do you think that there are so many defacements coming out of Brazil? Social Conditions? Politics?

A. I don't think that politics or social conditions are the reason. Many groups protest against the government, but they don't even know what they are talking about. They use this as an excuse. The principle reason is to show off. The reason for so many defacements coming out of Brazil is the facility with which we can learn here. Anyone with a minimum of programming knowledge can invade sites at will.

Q. What is the reason that your group defaces sites? What do you expect to gain from this?

A. To test our knowledge, to try and get some $$$ [cash], and like any other group, for fame as well. Perhaps we will be criticized for saying this, but it is true. Sometimes we do this [deface sites] with the objective of protesting against a company, an institution, or organization, but these cases are rare.

Q. What is your favorite Operating System, for home, for hacking, and for work?

A. We use mainly Windows, Linux, Solaris, and Mac. To 'play' at home I think that Windows is really good. To 'hack', it doesn't matter. We create remote shells for this purpose. For work, we prefer open source systems, like Linux, due to their low maintenance cost, and because they are Freeware. The fact that they include Source Code is an important factor as well, that way we know that we can trust in them. With Windows… well… we never know what our 'friends' at Microsoft put into it.

Q. By looking at your defacements, it appears that you have a preference for hacking Windows boxes, is there a reason for this?

A. We try to attack famous sites, or sites with some importance, as opposed to sub-domains from countries that no one has ever heard of. Finding holes in famous sites running *nix is difficult. That is the reason why we invade so many Windows boxes. We generally also invade not so famous Linux sites, or sites that already have been hacked, with the objective of creating shells, but in these cases we don't even deface the sites.

Q. Do the majority of holes that you find already have patches?

A. Yes. In a certain manner, there does not exist bugs that cannot be patched. Certain bugs in FTP's that we find, do not have patches, but this is the direct result of the admins neglect, and they could easily be corrected.

Q. What is the most common vulnerability that you come across?

A. Unicode, printer, and bugs in FTP's.

Q. If you had to choose just one tool for hacking, what would it be?

A. A book containing detailed information on all operating systems and vulnerabilities.

Q. What is your best advice to system administrators?

A. Visit sites dedicated to providing information about hackers and vulnerabilities, try and make contact with famous defacers, and always seek out new patches and updates.

Q. Do you work with other international groups? Did you participate in project China or something similar?

A. No, we have not participated in any 'project' but we do keep in touch with international groups.

Q. What is the average age of your members?

A. The age of our members ranges from 15 to 18 years old.

End of Interview with Perfect.br

On the surface, these Brazilian groups do appear to pose a serious threat to the global network infrastructure. In essence, however, there is a deeper message. These groups are mainly exploiting known vulnerabilities and poorly configured servers.

According to both Perfect.br and Prime Suspectz, the most common vulnerabilities they come across are: Unicode vulnerability, the cgi decode bug, and bugs in FTP servers and printers.

First up, the Unicode vulnerability, known also as: Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability, has been known since October 17, 2000. The Bugtraq ID for this vulnerability is: 1806. The Patches for this vulnerability can be found at[32]:

> From: < http://www.securityfocus.com/bid/1806 >
>
> IIS 4.0
> http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp
>
> IIS 5.0
> http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Microsoft Personal Web Server 4.0:

David Raitzer patch pws_patch.zip
http://www.geocities.com/p_w_server/pws_patch/index.htm

The cgi decode bug, also known as MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability. The Bugtraq ID for this vulnerability is: 2708. This vulnerability has the following patches available, according to Securityfocus.com[33]:

From < http://www.securityfocus.com/bid/2708 >

Microsoft IIS 5.0:

Microsoft patch Q293826_W2K_SP3_x86_en
http://download.microsoft.com/download/win2000platform/Patch/q293826/NT5/EN-US/Q293826_W2K_SP3_x86_en.EXE

Microsoft IIS 4.0:

Microsoft patch Q295534i
http://download.microsoft.com/download/winntsp/Patch/q293826/NT4/EN-US/Q295534i.exe

As far as incorrectly configured FTP servers, I recommend that system administrators first check the FTP Server vendors' site for patches and upgrades. Once all patches and upgrades are applied, read through the information that the vendor supplies regarding secure configuration.

I also recommend that system administrators purchase the Step-by-Step Guides from the Sans Institute [http://www.sansstore.org]. These excellent guides are written by top security professionals, and include information vital to securing Windows NT 4.0 and 2000, Solaris, and Linux.

The Brazilian groups I interviewed and analyzed have given systems administrators and security professionals the best advice possible: keep up to date on all the latest vulnerabilities, upgrades and patches, and follow security news closely.

The CIA will continue to view China and Russia as its greatest cyber threats. Through this study, the Brazilian connection has been brought to light. These groups do harbor the potential for great damage; however, preventative maintenance and security awareness can protect us from most of the attacks. Perhaps in the future, security will play a bigger role in software development, and technical education, but until then we must continue to do our part in securing the global network infrastructure.

References*

Jaques, Robert. "Hackers crack four Microsoft sites". 22 June 2001. http://webserv.vnunet.com/News/1123410 (22 June 2001)

Encyclopedia Britannica Online. Brazil. http://www.britannica.com/eb/article?eu=108679&tocid=0 (July 1, 2001)

Safemode.org. "! Sorted defacer records + top 50 most active defacers!" http://www.safemode.org/defacers   (July 13)

Leyden, John. "CIA admits it can't keep up with 'commie' hackers". 22 June 2001. http://www.theregister.co.uk/content/8/19906.html (23 June 2001)

Bertholdo , Leandro Marcio. "Polícia identifica mais um hacker do Inferno.br". 31 March 2000. http://www.cert-rs.tche.br/listas/infoseg/msg00102.html (23 June 2001)

Alldas.de. "Alldas.de defacement archive". http://defaced.alldas.de (July 13, 2001)

DIN - Deutches Institut für Normung e.V. "English country names and code elements". http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en listp1.html. (July 12, 2001)

Security Focus. "Microsoft IIS and PWS Extended Unicode Directory Transversal Vulnerability." http://www.securityfocus.com/bid/1806

Security Focus. "MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability". http://www.securityfocus.com/bid/2708

Alldas.de. “Attacker Statistics for Prime Suspectz” http://defaced.alldas.de/defaced.php?attacker=Prime+Suspectz&p=1 (July 13)

Alldas.de. “Attacker Statistics for Perfect.br” http://defaced.alldas.de/defaced.php?attacker=Perfect.BR&p=1 (July 13)

Alldas.de. “Attacker Statistics for Perfect.br” http://defaced.alldas.de/defaced.php?attacker=BHS&p=1 (July 13)

Alldas.de. “BHS Defacement”. http://defaced.alldas.de/mirror/2001/06/30/www.retas.camcom.it/ (July 13)

Alldas.de. “BHS Defacement”. http://defaced.alldas.de/mirror/2001/07/04/heatweb.edim.com.my/ (July 13)

Alldas.de. “Prime Suspectz Defacement”. http://defaced.alldas.de/mirror/2001/04/28/www.intacglobalinvestments.com/ (July 13)

Alldas.de. “Prime Suspectz Defacement”. http://defaced.alldas.de/mirror/2001/06/21/redsand.rte.microsoft.com/ (July 13)

Alldas.de. “Prime Suspectz Defacement”. http://defaced.alldas.de/mirror/2001/06/21/feeds.mobile.msn.com/ (July 7)

Alldas.de. “Prime Suspectz Defacement”. http://defaced.alldas.de/mirror/2001/06/21/arulk.rte.microsoft.com/ (July 13)

Alldas.de. “Prime Suspectz Defacement”. http://defaced.alldas.de/mirror/2001/06/22/webcfeedback.msn.com/ (July 7)

Alldas.de. “Perfect.BR Defacement”. http://defaced.alldas.de/mirror/2001/07/06/www.budhughes.com/ (July 13)

*****Note on URL’s: Alldas.de is a dynamic site; as the quantity of defacements increases the pages reflect these increases. Also

Alldas.de has been suffering dDOS attacks over the past couple weeks. All links included here are valid links.

End Notes

[1] Jaques, Robert. “Hackers crack four Microsoft sites”. 22 June 2001. http://webserv.vnunet.com/News/1123410 (22 June 2001)
[2] Encyclopedia Britannica Online. “Brazil” http://www.britannica.com/eb/article?eu=108679&tocid=0 (July 1, 2001)
[3] Safemode.org. “! Sorted defacer records + top 50 most active defacers!” *http://www.safemode.org/defacers (July 5)*
[4] Leyden, John. “CIA admits it can't keep up with 'commie' hackers”. 22 June 2001. http://www.theregister.co.uk/content/8/19906.html (23 June 2001)
[5] Bertholdo , Leandro Marcio. http://www.cert-rs.tche.br/listas/infoseg/msg00102.html (23 June 2001)
[6] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=Prime+Suspectz&p=1 ; http://defaced.alldas.de/defaced.php?attacker=Perfect.BR&p=1; and http://defaced.alldas.de/defaced.php?attacker=BHS&p=1 (July 13)
[7] BHS Defacement Image. http://defaced.alldas.de/mirror/2001/06/30/www.retas.camcom.it/ (July 13)
[8] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=BHS&op=details (July 13)
[9] Safemode.org. “! Sorted defacer records + top 50 most active defacers!” *http://www.safemode.org/defacers (July 13)*
[10] Safemode.org. “! Sorted defacer records + top 50 most active defacers!” *http://www.safemode.org/defacers (July 13)*

[11] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=BHS&p=1 (July 5)
[12] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=BHS&p=1 (July 5)
[13] DIN. Deutches Institut für Normung e.V. “English country names and code elements”. http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html
[14] BHS Defacement. http://defaced.alldas.de/mirror/2001/07/04/heatweb.edim.com.my/ (July 13)
[15] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=BHS&op=details (July 13)
[16] Prime Suspectz Defacement Image. http://defaced.alldas.de/mirror/2001/04/28/www.intacglobalinvestments.com/ (July 13)
[17] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=Prime+Suspectz&op=details (July 13)
[18] Safemode.org. “! Sorted defacer records + top 50 most active defacers!” *http://www.safemode.org/defacers (July 13)*
[19] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=Prime+Suspectz&p=1

[20] Prime Suspectz Defacement. http://defaced.alldas.de/mirror/2001/06/21/redsand.rte.microsoft.com/ (July 7)

[21] Prime Suspectz Defacement. http://defaced.alldas.de/mirror/2001/06/21/feeds.mobile.msn.com/ (July 7)

[22] Prime Suspectz Defacement. http://defaced.alldas.de/mirror/2001/06/21/arulk.rte.microsoft.com/ (July 13)

[23] Prime Suspectz Defacement. http://defaced.alldas.de/mirror/2001/06/22/webcfeedback.msn.com/ (July 7)

[24] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=Prime+Suspectz&op=details (July 13)

[25] Perfect.BR Defacement Image.

[26] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=Perfect.br&op=details

[27] Safemode.org. "! Sorted defacer records + top 50 most active defacers!" *http://www.safemode.org/defacers (July 13)*

[28] Safemode.org. *http://www.safemode.org/defacers (July 5)*

[29] Perfect.BR Defacement. http://defaced.alldas.de/mirror/2001/07/06/www.budhughes.com/ (July 13)

[30] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=Perfect.BR&p=1 (July 13)

[31] Alldas.de. http://defaced.alldas.de/defaced.php?attacker=Perfect.br&op=details (July 13)

[32] Security Focus. "Microsoft IIS and PWS Extended Unicode Directory Transversal Vulnerability." http://www.securityfocus.com/bid/1806 (July 5)

[33] Security Focus. "MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability". http://www.securityfocus.com/bid/2708 (July 5)