Crimeware Related to Brazilian Frauds

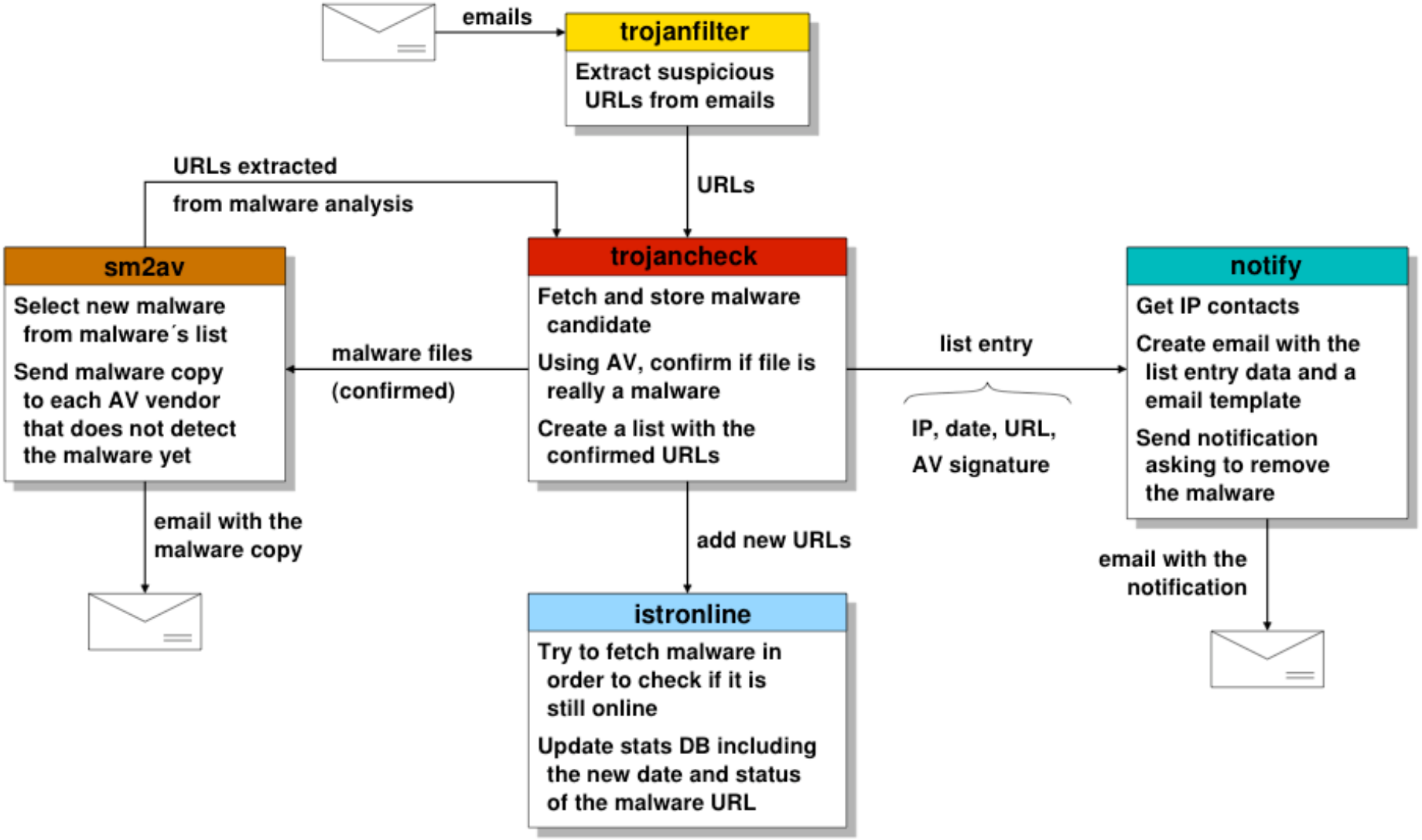
Cristine Hoepers
cristine@cert.br

CERT.br – Computer Emergency Response Team Brazil
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee

Agenda

- How the data is collected and processed
- Some statistics
- AntiVirus vendors detection rates
- Indicators of defense software usage in Brazil

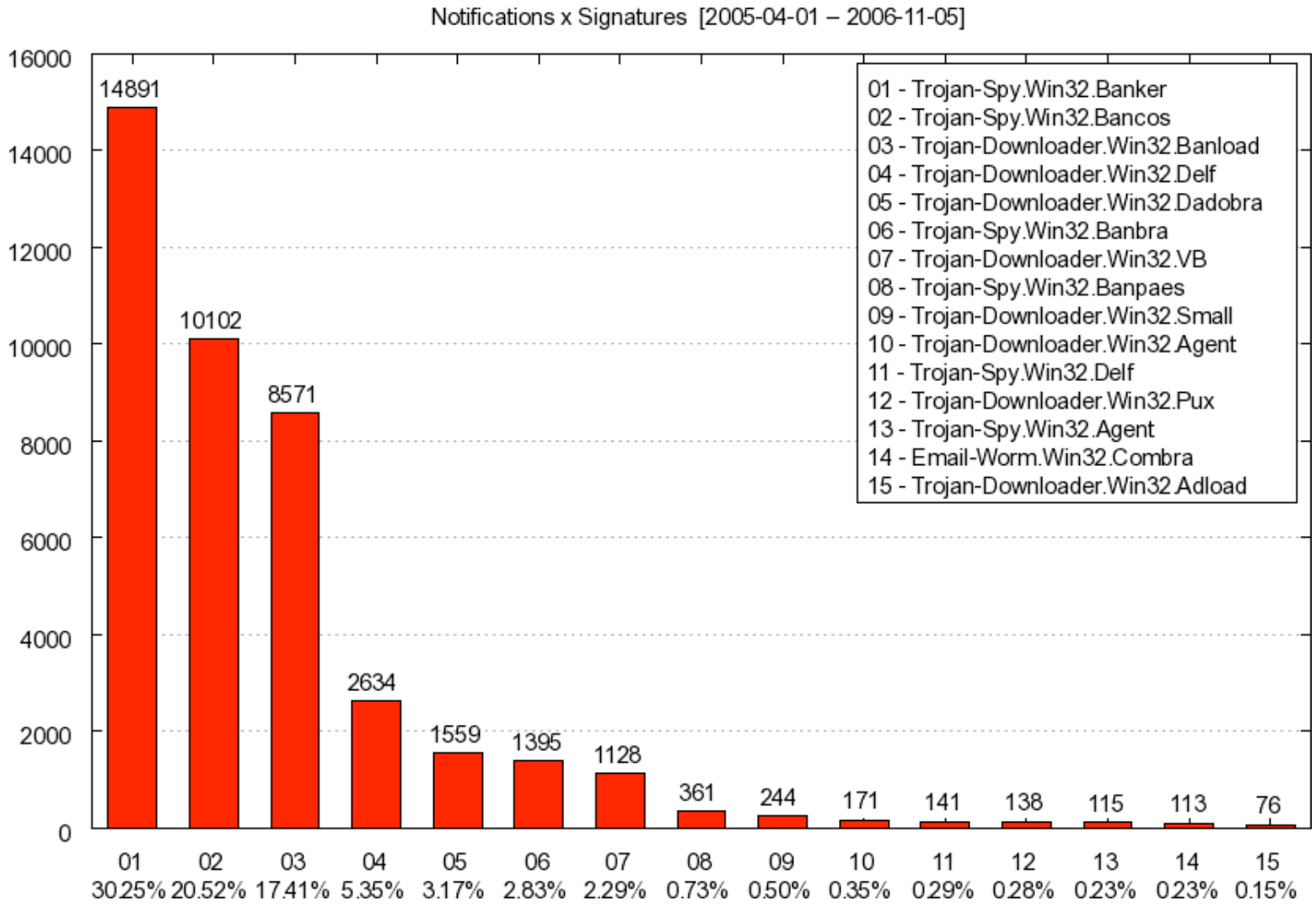
Overview of the System that Processes the Malware



Statistics: April 1st, 2005 - November 3rd, 2006

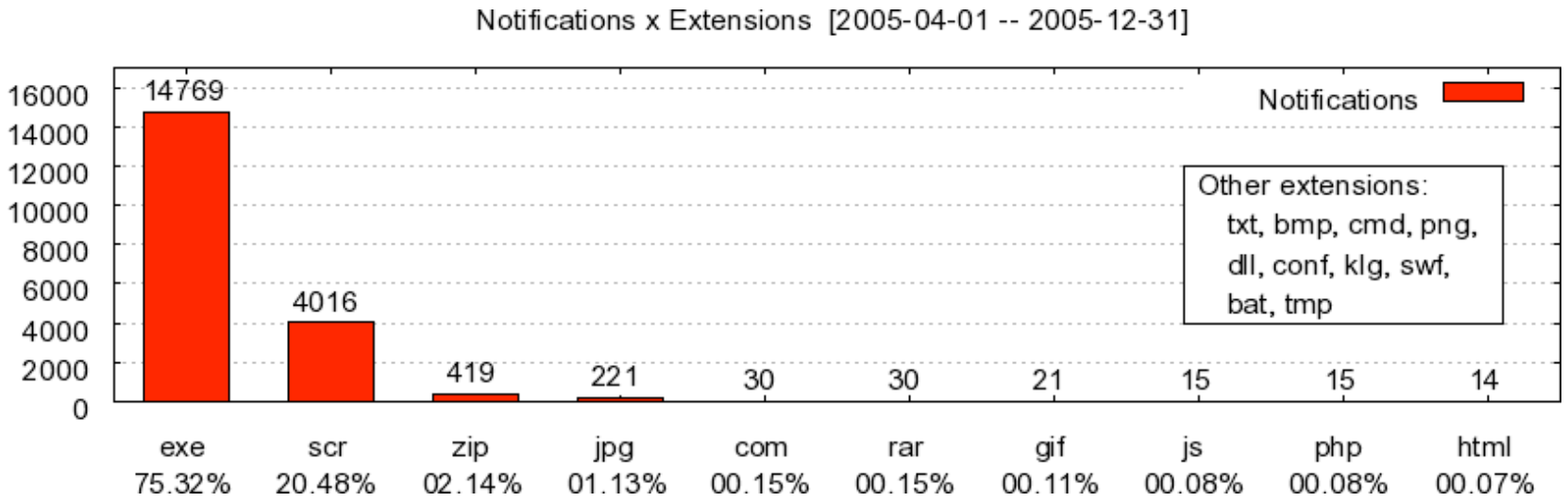
Category	Total
Unique URLs	36069
Hosts	11940
Domains	6886
Contacts for the domains/networks	2741
IP Addresses	5054
IP Allocation's Country Codes	76
Unique trojan samples (unique hashes)	28350
Trojans' file names	15157
File Extensions	78
AntiVirus signatures (unique)	2623
AntiVirus signatures (grouped by "family")	173
Email notifications sent by CERT.br	25922

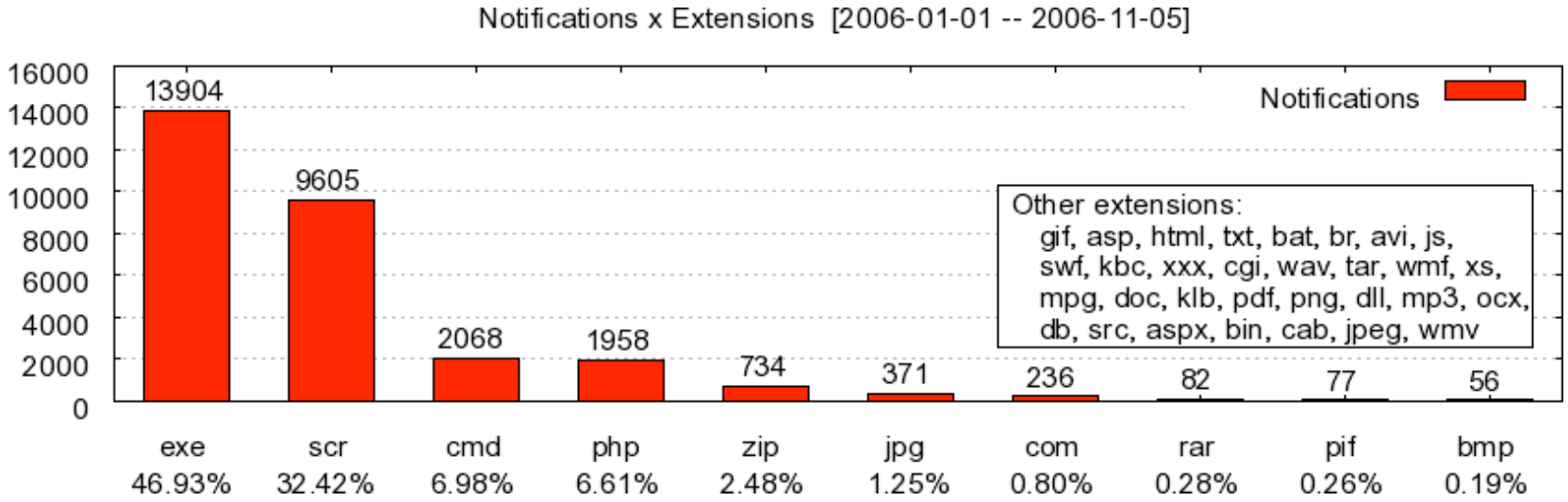
Top 15 Signature “Families”



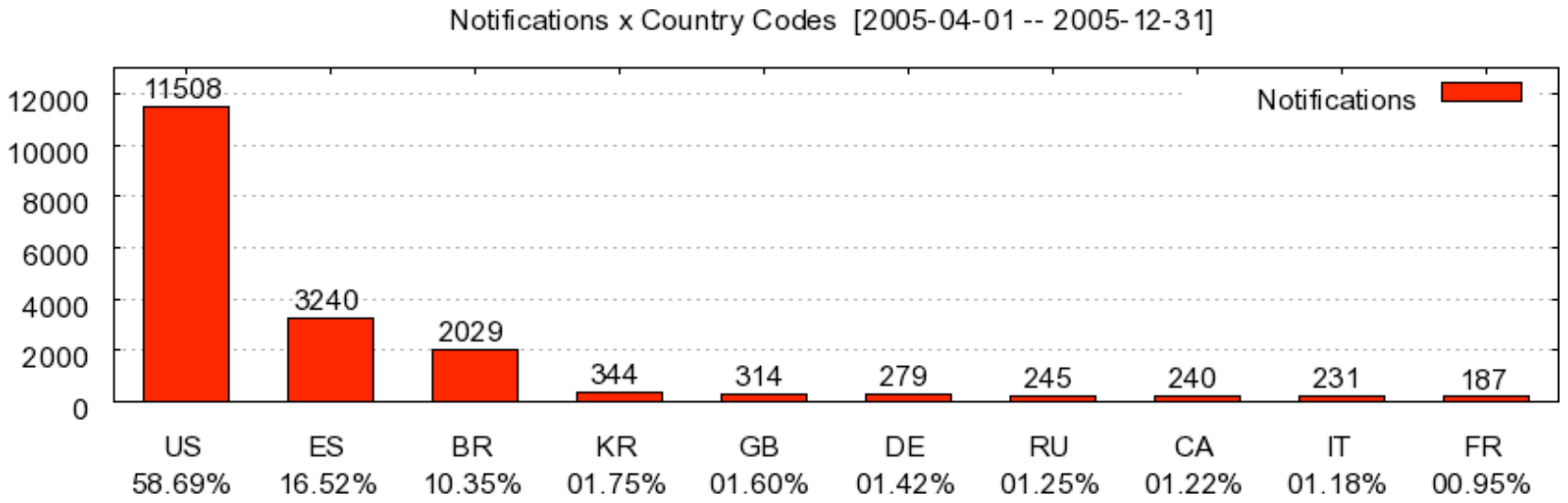
Signatures from Kaspersky Lab.

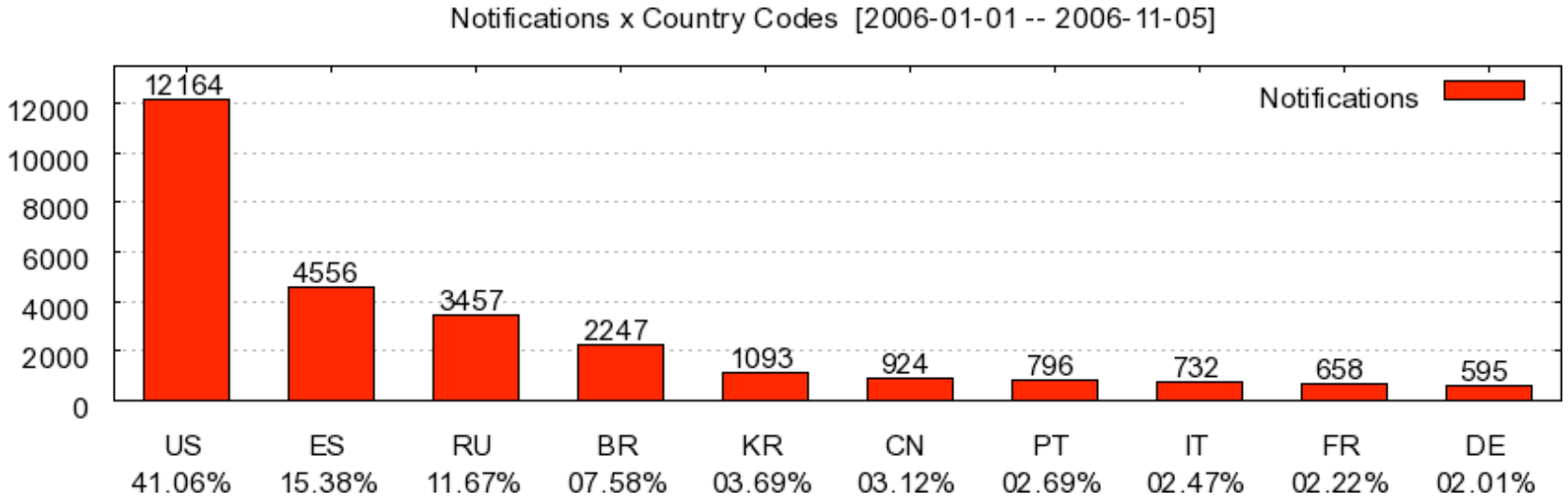
File Extensions





IPs Hosting Malware - RIRs Allocation Information





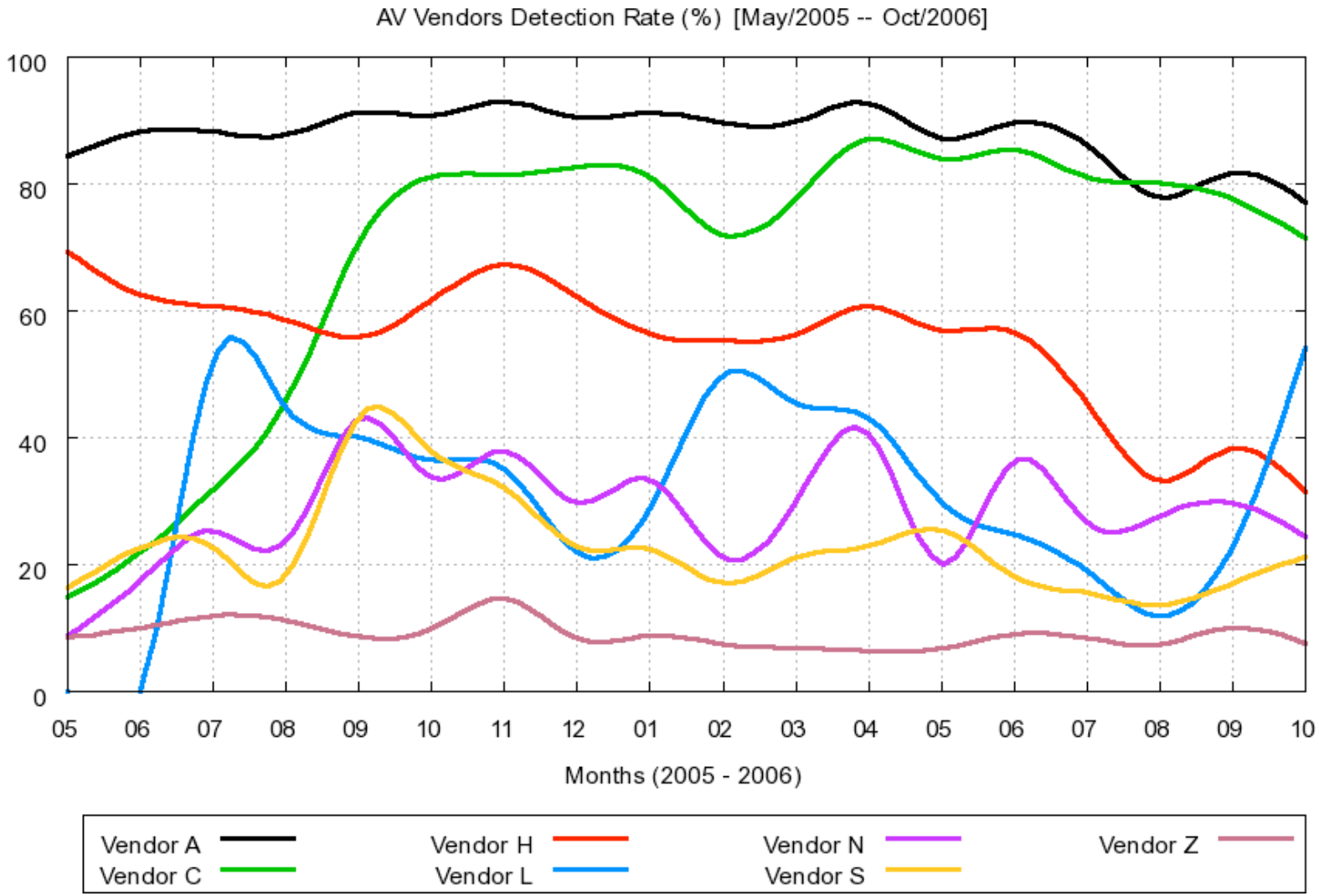
AntiVirus Detection Rate: April 1st, 2005 - November 5th, 2006

Antivirus Vendor	Samples Tested	Samples not detected	Samples Detected	Detection Rate (%)
Vendor A	28315	3505	24810	87.62
Vendor B	5651	1019	4632	81.97
Vendor C	28349	8776	19573	69.04
Vendor D	28165	9417	18748	66.56
Vendor E	28331	9473	18858	66.56
Vendor F	2611	921	1690	64.73
Vendor G	28041	11369	16672	59.46
Vendor H	28350	12745	15605	55.04
Vendor I	17160	8722	8438	49.17
Vendor K	17888	10846	7042	39.37
Vendor L	24284	15957	8327	34.29
Vendor N	28038	19891	8147	29.06
Vendor O	27983	20019	7964	28.46
Vendor P	28339	20340	7999	28.23
Vendor Q	23811	17167	6644	27.90
Vendor T	28190	21938	6252	22.18
Vendor Z	26881	24430	2451	9.12

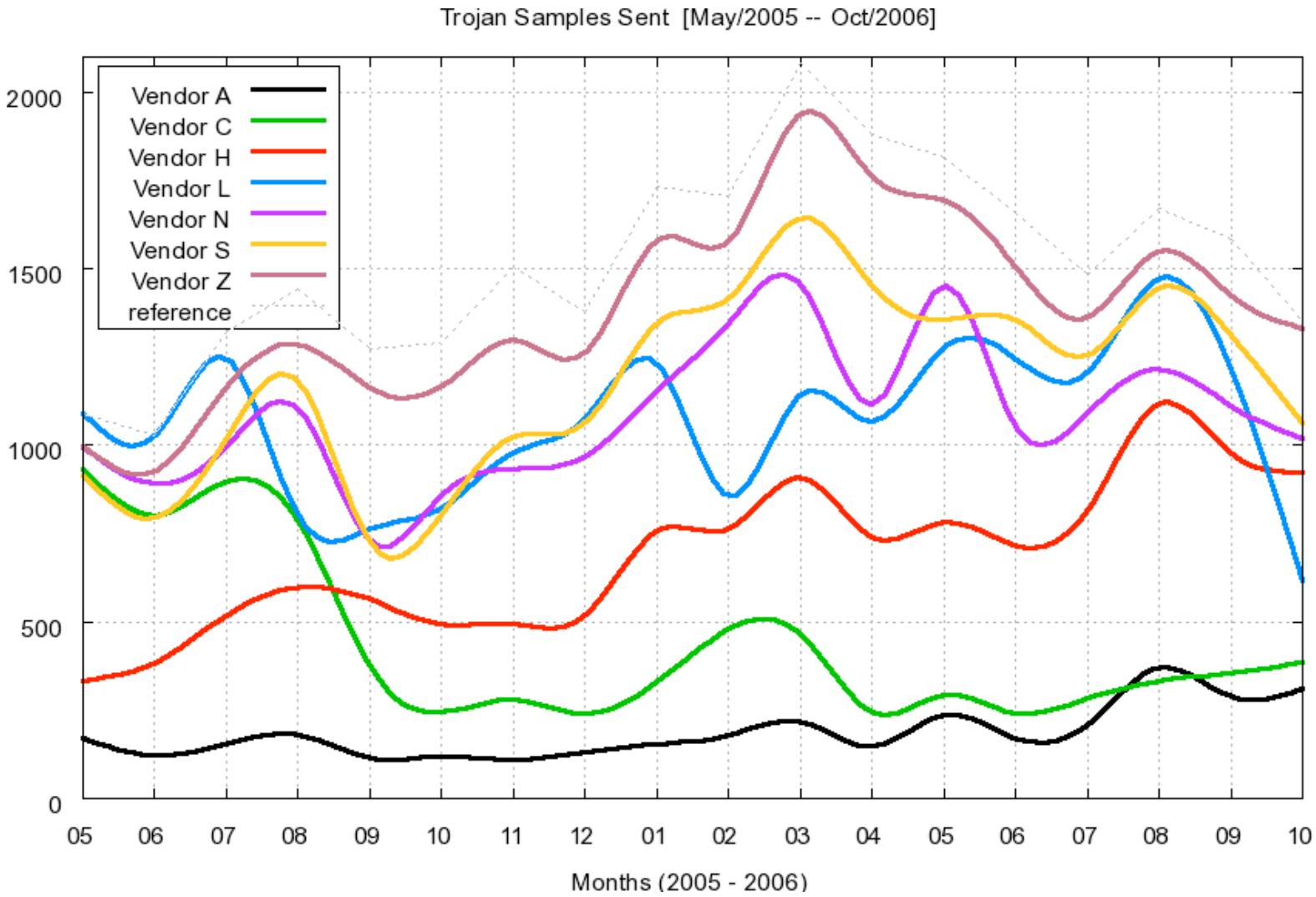
Only **2** vendors with the detection rate above **80%**

~70% of vendors with less than **40%**

Detection Rate - Monthly



Trojan Samples Sent - Monthly



National survey conducted by CGI.br in August 2005

F1 - Security problems faced using the Internet

Percentage over the number of individuals who used the Internet in the 3 months prior to the survey

	None	Virus (un-authorized access)	Virus (software or hardware damage)	Abuse of personal information	Financial Fraud	Other	Don't Remeber
Total	40,99	19,64	7,13	1,67	0,94	1,10	0,24

F2 - Computer security measures adopted

Percentage over the number of individuals who have Internet access at home

	Anti-Virus	Personal Firewall	Anti-spyware Software
Total	69,76	19,33	22,09

F3 - Anti-Virus updating frequency

Percentage over the number of individuals who have Internet access at home

	Daily	Weekly	Monthly	Every 3 Months	Didn't Update
Total	21,11	27,01	17,37	3,47	31,03

Notes -- *number of individuals who used the Internet in the 3 months prior to the survey: ~44 million people*
number of individuals who have internet access at home: ~17 million people

Additional References

- This presentation
  http://www.cert.br/docs/presentations/

- CGI.br - Brazilian National Survey on ICT
  http://www.nic.br/indicadores/

- CERT.br
  Computer Emergency Response Team Brazil
  http://www.cert.br/