“Internet Background Noise” or analyzing data garbage

Text: Rolf Gartmann, SWITCH, gartmann@switch.ch

What the benefits of collecting Internet data garbage can be and why the hunter-gatherer approach helps to identify anomalies, problems and misuse of the network and systems.

Recycling – a word, a process we get in touch in our daily life. But have you ever thought about recycling data garbage? What about all those data packets on the Internet, which are for whatever reason sent to unused IP addresses and could be tagged as data garbage? Why not collect and analyse these packets and gain useful information? Based on these thoughts, SWITCH-CERT (Computer Emergency Response Team) started a project named “Internet Background Noise” (IBN). The definition for “data garbage” we use in this environment: packets on the network, which are targeted towards unused IP addresses.

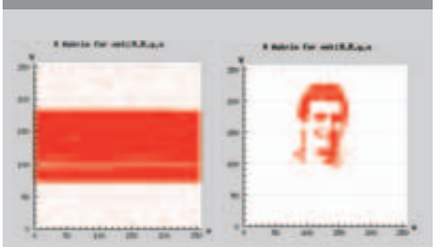
Based on that definition a sensor was set up, which collects these packets and allows further processing and visualization. In principal there shouldn’t arrive a single packet at that sensor, because by definition it only collects packets with unused destination addresses. Therefore every single, seen packet is some kind of data garbage. The reason of seeing packets at all can be interpreted as: misconfiguration of components (systems, routers), scanning activities, outbreak of worms, backscatter activities from “Denial of Service” attacks (due to spoofed source IP addresses) and so on. The processed information can be used to inform our customers about infected systems, as some sort of early warning system, as a basis for statistical data analysis and as a local Internet weather map, which shows the current status of mostly abusive/abnormal network activity. Analysis of the collected data is currently based on the IP protocols TCP, UDP and ICMP, source and destination addresses and destination ports, respectively types in case of ICMP.

IBN is an additional piece of a puzzle in the daily information gathering process within a CERT

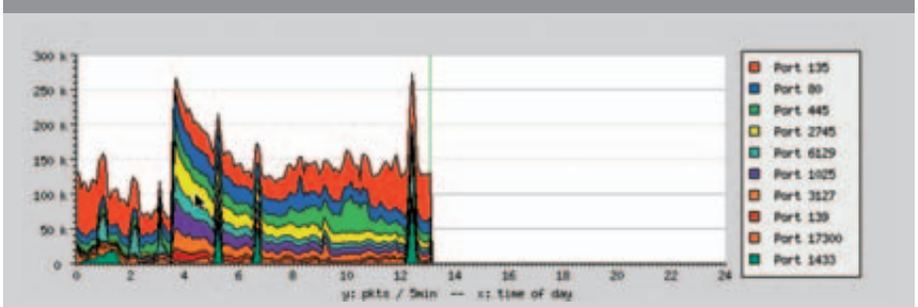
Part of the collected, current data is publicly available at http://www.switch.ch/security/services/IBN. For example the illustration of TCP port statistics dated 2004/04/05 around 1.00 p.m. shows a unique pattern of port 80, 445, 2745, 6129, 1025 and 3127 scanning activities. Further analysis revealed a distributed scan for different current vulnerabilities and misconfigurations: open shares, already installed backdoors from latest viruses, remote administration tool vulnerability.

The collected data can also be used for different visualizations, e.g. based on the performed scanning pattern against the unused address space, which is shown in the IBN matrix plots below: a common and an obviously artificial one.

IBN Matrix Plots



TCP Port Statistics



Rolf Gartmann works as Network Security Engineer at SWITCH. In his work he is involved in Computer Incident Handling issues, Computer and Network Security measurements and is member of different national and international forums like FIRST, TF-CSIRT and SWIRT.

Furthermore the IBN sensor also helps to get more and timely information about outbreaks of worms and latest exploits (e. g. witty worm). Overall, IBN can be regarded as an additional piece of a puzzle in the daily information gathering process within a CERT.

References

SWITCH IBN:
http://www.switch.ch/security/services/IBN

Similar projects:
- CAIDA: Network Telescope: http://www.caida.org/analysis/security/telescope/
- The Riverhead/IUCC Internet Telescope: http://noc.ilan.net.il/research/riverhead/
- iSink: http://www.potaroo.net/iepg/july-2003/isink.pdf

Analysis of Witty worm:
http://www.caida.org/analysis/security/witty/

SWITCH-CERT:
http://www.switch.ch/cert/