Getting back at Trudy

SSH Botnet Member Credential Collection
using
Connect Back Honeypots

Tobias Fiebig

University of Amsterdam

01/08/2013

The Problem...

- SSH-Bruteforcing.
- Systems on the internet trying to authenticate to your system with all kinds of stupid usernames and passwords.

Ok, hands up...

- Ok? Who had the problem of being owned by an SSH-Bruteforcer?

Ok, hands up...

- Ok? Who had the problem of being owned by an SSH-Bruteforcer?
- Ok, lets ask differently... Who knows somebody who has a friend whose father in law's dog once had this problem... ?

Honestly... hit me as well...

From: Intrusion Detection Team <idt@[redacted]navy.mil>
To: abuse@wybt.net
Subject: hacker activity 195.191.196.[redacted]
Date: [redacted]2012 [redacted]

This email is for your information. It is *not* a request
for any specific action. It was automatically generated,
but all replies will be handled personally.

A host/port sweep

20[redacted]
TCP Port 22 Sweep of OUR subnet(s):
198.[redacted]
FROM 195.191.196.[redacted] ([redacted]wybt.net [DE]))
Starttime [redacted]; Endtime [redacted]
TCP Port 22: attempts on about 76 addresses.

was logged at this United States Department of Defense facility,
apparently originating from one of your machines. The time zone is
PDT (Greenwich -7 hours).

Suggested interpretations:
1. One of your machines has been compromised/infected and is scanning
our networks.
2. One of your users is scanning our networks.

Thank you for your attention.

--Intrusion Detection Team
idt@[redacted].navy.mil
[redacted]

Where do these systems come from?

Where do these systems come from?

- Probably not the attackers homebox...

Where do these systems come from?

- Probably not the attackers homebox...
- But what kind of system could such an attacker have at his disposal?

Where do these systems come from?

- Probably not the attackers homebox...
- But what kind of system could such an attacker have at his disposal?
- Yes, systems they penetrated by Bruteforcing the SSH daemon...

What do we know about these systems?

What do we know about these systems?

- You get detected if you change the password.

What do we know about these systems?

- You get detected if you change the password.
- The password that is used, is probably in the attackers wordlist.

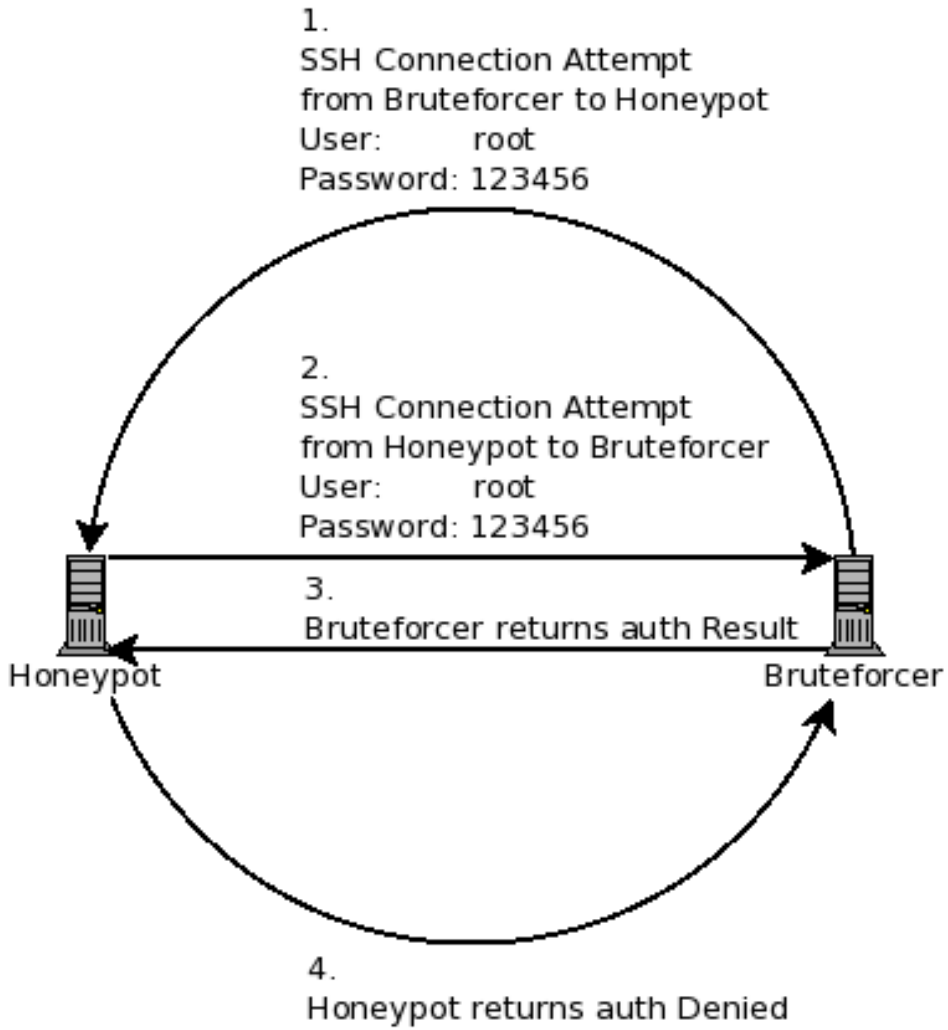
What do we know about these systems?

- You get detected if you change the password.
- The password that is used, is probably in the attackers wordlist.
- The attacker runs his SSH Bruteforcing Software on that machine.

What do we know about these systems?

- You get detected if you change the password.
- The password that is used, is probably in the attackers wordlist.
- The attacker runs his SSH Bruteforcing Software on that machine.
- Wait... what?

Research Question: Does this work?



Ethical Implications

- Subjects may be unaware of infection/participation in the research.

Ethical Implications

- Subjects may be unaware of infection/participation in the research.
  - Inform subjects. Has been done via appropriate channels.

Ethical Implications

- Subjects may be unaware of infection/participation in the research.
  - Inform subjects. Has been done via appropriate channels.
- Gathered data is pretty sensitive.

Ethical Implications

- Subjects may be unaware of infection/participation in the research.
  - Inform subjects. Has been done via appropriate channels.
- Gathered data is pretty sensitive.
  - Fully anonymize data before publication.

Legal Implications

- Different jurisdictions touched.
- In nearly all cases: Unauthorized logins prohibited by applicable law.

Legal Implications

- Different jurisdictions touched.
- In nearly all cases: Unauthorized logins prohibited by applicable law.
  - $\rightarrow$ Do not login, just authenticate.

Just quickly thrown together...

- Something that can:

Just quickly thrown together...

- Something that can:‘
  - Provide an SSH server.

Just quickly thrown together...

- Something that can:‘
  - Provide an SSH server.
  - Get Username/Password combinations

Just quickly thrown together...

- Something that can:‘
  - Provide an SSH server.
  - Get Username/Password combinations
  - Try to authenticate to the remote SSH server, without opening a session.

Paramiko to the Rescue!

- Based on the Open Source python ssh library paramiko[1] and the demo SSH server provided with it.
- Patched for threading, multiple simultanious connections, providing an Ubuntu 12.04-style banner and the connect-back feature.
- Basically: 165 lines of python code after patching.

[1] http://www.lag.net/paramiko/

Just with a few hosts...

- 8 Hosts
- 4 Countries, Two Continents, 8 AS
- All systems listened with the sshcb software on port 22
- Ran for appr. 2 weeks

... and with some /24s.

- 8 /24 subnets from different /16
  - 6 from RIPE as temporary assignement
  - 1 from SNE/SURFnet
  - 1 from WYBT.net
- Each networks port 22 and ICMP DNATed to one box listening with the sshcb software on port 22
- Also ran for appr. 2 weeks

Single Host Study

Host	Avg. Connections/h	Max Connections/h	Total Connections
All	232.06	3063	69386
p2o1	26.96	1136	8062
p2o2	18.46	746	5519
p2o3	24.97	1219	7467
p2o4	19.68	645	5886
p2o5	25.81	793	7716
p2o6	41.40	1560	12379
p2o7	35.11	717	10497
p2o8	39.67	3042	11860

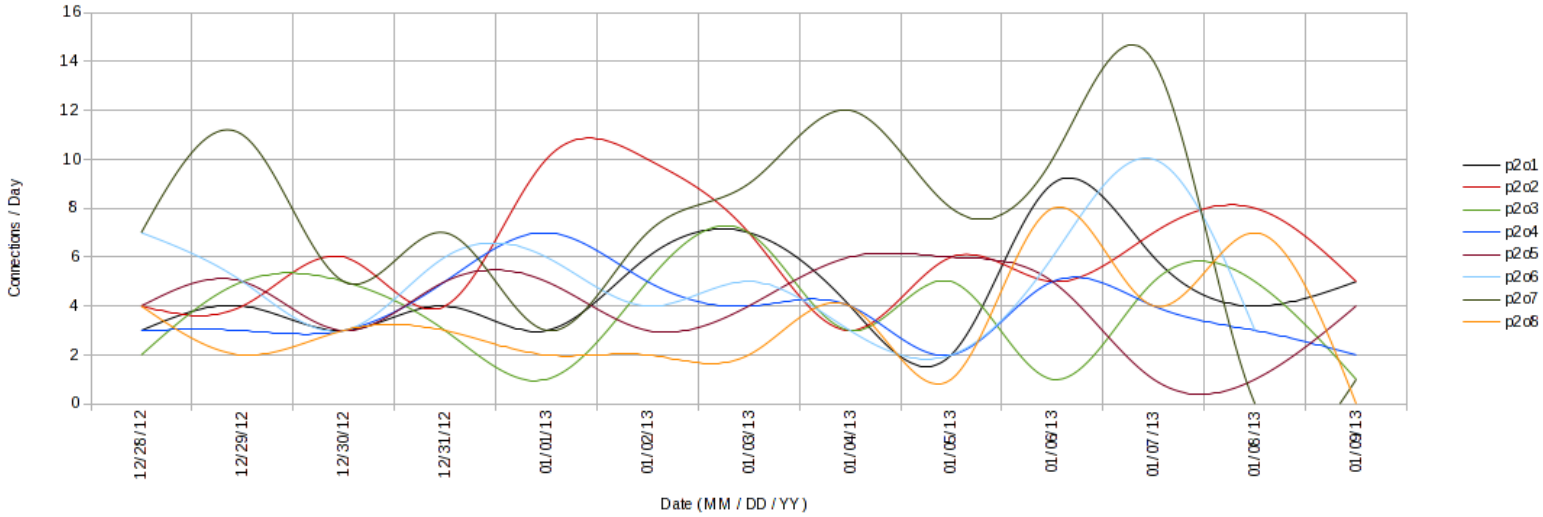
Table: Base Data for Single Host Study

Single Host Study

Host	Penetrated Hosts	Non Penetrated Hosts	Successrate
All	30	290	9.38%
p2o1	2	49	3.92%
p2o2	8	65	10.96%
p2o3	1	42	2.33%
p2o4	1	37	2.63%
p2o5	4	43	8.51%
p2o6	6	53	10.17%
p2o7	4	58	6.45%
p2o8	4	36	10.00%

Table: Success Rate for Single Host Study

Single Host Study - Graph



Network Study

Net	Avg. Connections/h	Max Connections/h	Total Connections
All	1993.72	33027	663912
145.100.109.0/24	668.87	25202	222736
151.216.20.0/24	182.19	3598	60670
151.217.0.0/24	173.47	8294	57767
151.220.0.0/24	211.29	8186	70361
151.221.0.0/24	192.38	8218	64064
151.222.0.0/24	175.58	3740	58470
151.223.0.0/24	196.59	8296	65466
195.191.197.0/24	193.32	3468	64378

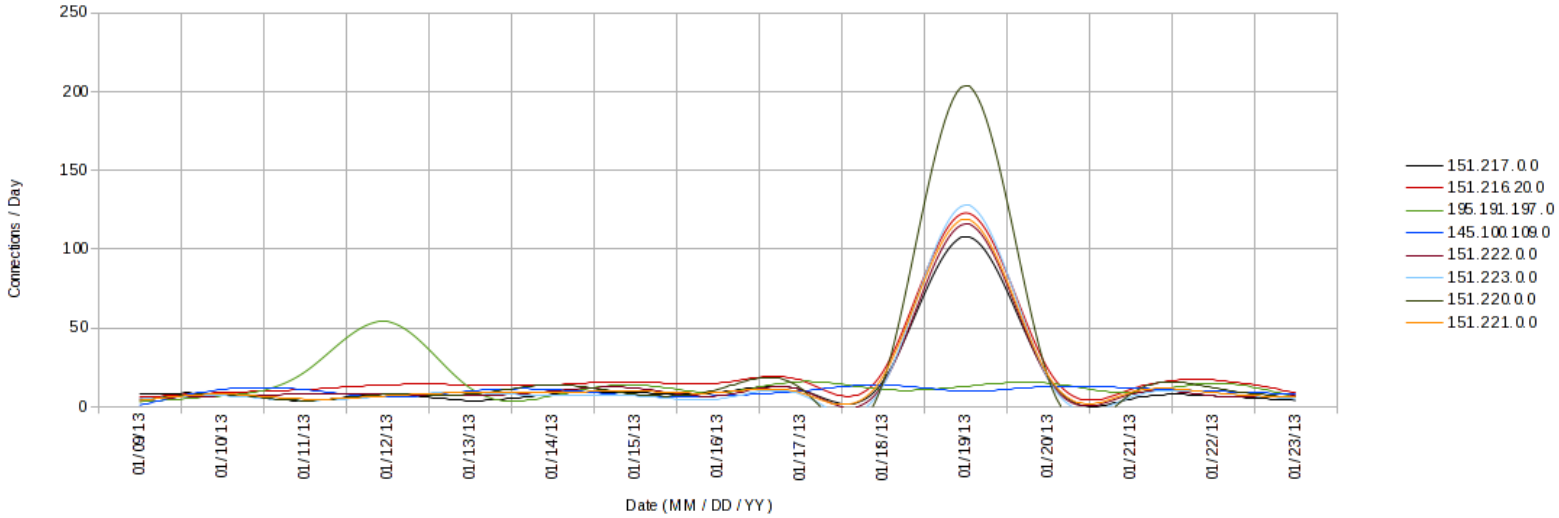
Table: Base Data for Network Study

Network Study

Net	Penetrated Hosts	Non Penetrated Hosts	Successrate
All	36	632	5.38%
145.100.109.0/24	14	74	15.91%
151.216.20.0/24	13	257	4.81%
151.217.0.0/24	11	180	5.76%
151.220.0.0/24	12	287	4.01%
151.221.0.0/24	8	202	3.81%
151.222.0.0/24	9	193	4.46%
151.223.0.0/24	8	201	3.83%
195.191.197.0/24	4	158	2.47%

Table: Success Rate for Network Study

Network Study - Graph



Network Study

Net	Avg. Connections/h	Max Connections/h	Total Connections
All	1732.44	33027	576901
145.100.109.0/24	668.88	25202	222736
151.216.20.0/24	140.88	3598	46913
151.217.0.0/24	136.90	8294	45587
151.220.0.0/24	176.31	8186	58710
151.221.0.0/24	161.26	8218	53698
151.222.0.0/24	135.40	3696	45089
151.223.0.0/24	156.77	8296	52204
195.191.197.0/24	156.05	3468	51964

Table: Base Data for Network Study - outliers filtered

Network Study

Net	Penetrated Hosts	Non Penetrated Hosts	Successrate
All	35	260	11.86%
145.100.109.0/24	14	74	15.91%
151.216.20.0/24	12	148	7.50%
151.217.0.0/24	10	83	10.75%
151.220.0.0/24	11	93	10.58%
151.221.0.0/24	7	93	7.00%
151.222.0.0/24	8	89	8.25%
151.223.0.0/24	7	85	7.61%
195.191.197.0/24	4	113	3.42%

Table: Success Rate for Network Study - outliers filtered

Uncovered group passwords...

- Some passwords are not like other passwords. They are special.

Uncovered group passwords...

- Some passwords are not like other passwords. They are special.
- Example: “spargeosu#^%*&138cucapulinpicior”

Uncovered group passwords...

- Some passwords are not like other passwords. They are special.
- Example: “spargeosu#^%*&138cucapulinpicior”
- Successfull connect back attempts with those passwords.
- Probably belong to some Script-Kiddy group.

... and nationalities.

- “spargeosu#^%*&138cucapulinpicior”

... and nationalities.

- “spargeosu#^%*&138cucapulinpicior”
- Cosmin Dumitru tipped me of: that is Romanian.
- His translation: ”sparge osul” - break the bone. ”cu capul in picior” - with head struck by foot - or something like that.

Conclusion:

Conclusion:

People use good passwords:

Conclusion:

People use good passwords:✗

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗

A reasonable amount of hosts could be penetrated with this method:

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗

A reasonable amount of hosts could be penetrated with this method:✓

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗

A reasonable amount of hosts could be penetrated with this method:✓

Method works:

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗

A reasonable amount of hosts could be penetrated with this method:✓

Method works:✓

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗

A reasonable amount of hosts could be penetrated with this method:✓

Method works:✓

All data has been anonymized and published at `http://sshcb.wybt.net/`:

Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗

A reasonable amount of hosts could be penetrated with this method:✓

Method works:✓

All data has been anonymized and published at `http://sshcb.wybt.net/`:✓

Last remarks:

Thanks to all the people providing support, resources and even sponsoring!

Pieter Lexis - Told me to stop talking and test the theory.
Dr. Hans Dijkman - Gave huge support in solving the ethical and legal issues of this work.
Nadine Donaldson, BSc - Gave helpful advise on the data analysis.
Kay Rechthien - Assisted in setting up resources and networks.
Stefan Wahl - Supported the project by providing LIR services for the RIPE networks.
Niels Sijm, MSc - Assisted in setting up resources and networks.
Theodor Reppe - Provided systems for the single host study.

Greetings to **Elmo Todurov** from the University of Tallinn, who independently had the same idea during the finalisation of this research.