



Catch-22: Uncovering Compromised Hosts using SSH Public Keys

They can run but cannot hide...

Cristian Munteanu¹

Georgios Smaragdakis²

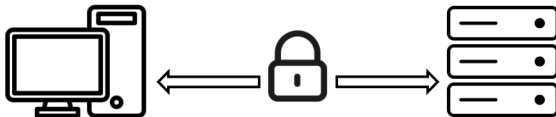
Anja Feldmann¹

*Tobias Fiebig*¹

¹Max-Planck Institut für Informatik ²TU Delft

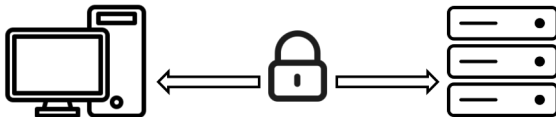


OpenSSH...



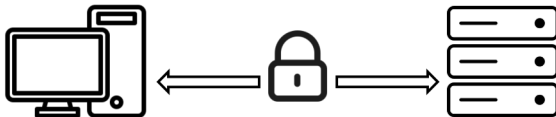
- When Telnet is not enough...
- No, you also can't use rsh...
- Has a tendency of inviting... guests

OpenSSH...



- When Telnet is not enough...
- No, you also can't use rsh...
- Has a tendency of inviting... guests

OpenSSH...



- When Telnet is not enough...
- No, you also can't use rsh...
- Has a tendency of inviting... guests

Guests bring presents, no?



```
> # cd ; chattr -ia .ssh; lockr -ia .ssh
> # cd && rm -rf .ssh && mkdir .ssh &&
echo "ssh-rsa AAAAB3.....+oRw== mdrfckr">>.ssh/authorized_keys &&
chmod -R go= /.ssh && cd
```

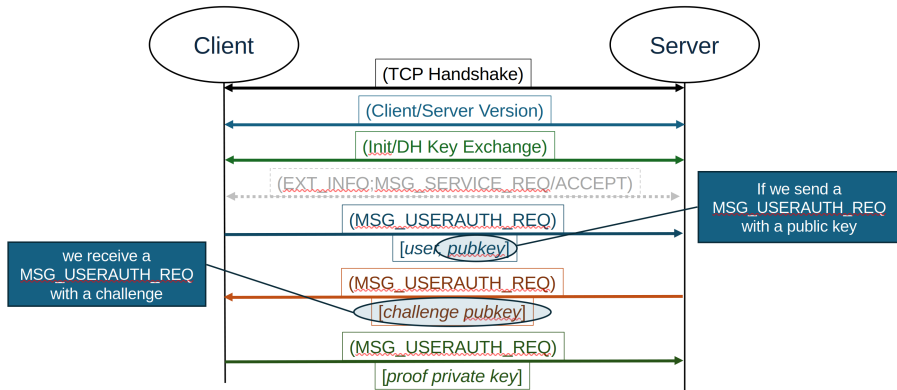
Guests bring presents!



```
> # cd ; chattr -ia .ssh; lockr -ia .ssh
> # cd && rm -rf .ssh && mkdir .ssh &&
echo "ssh-rsa AAAAB3.....+oRw== mdrfckr">>.ssh/authorized_keys &&
chmod -R go= /.ssh && cd
```



OpenSSH Authentication Procedure



<https://rushter.com/blog/public-ssh-keys/>



Does it work?



- Implemented as a Zgrab2 module
- Tested on:
 - OpenSSH v9.4-v2.1.1
 - Dropbear v0.84-v0.23
 - BitviseSSH v9-v6
 - WolfSSH v1.4

	Year	Censys (all ports) 2024-04-16	Our Scan (22, 2222) 2024-04-05	Censys (22, 2222) 2024-04-24	Deployment Zgrab	Zgrab2	Pubkey Login
OpenSSH:							
9.4	2024	<0.01%	<0.01%	<0.01%	✓	✓	✓
...	2016-2024	29.21%	22.7%	46.1%	✓	✓	✓
7.4	2016	23.01%	17.00%	18.08%	✓	✓	✓
...	2001-2016	22.28%	12.3%	6.17%	✓	✓	✓
3.0	2001	<0.01%	<0.01%	<0.01%	✓	✓	✓
2.9	2001	<0.01%	<0.01%	<0.01%	✓	✓	✗
...	2000-2001	<0.01%	<0.01%	<0.01%	✓	✓	✗
2.1.1	2000	<0.01%	<0.01%	<0.01%	✓	✓	✗
Dropbear:							
0.84	2024	<0.01%	<0.01%	<0.01%	✓	✓	✓
...	2019-2024	2.42%	0.91%	0.77%	✓	✓	✓
0.78	2019	8.36%	10.01%	12.74%	✓	✓	✓
...	2005-2019	3.51%	1.23%	3.80%	✓	✓	✓
0.47	2005	<0.01%	<0.01%	<0.01%	✓	✓	✓
0.46	2005	<0.01%	<0.01%	<0.01%	✗	✗	✗
...	2004-2005	<0.01%	<0.01%	<0.01%	✗	✗	✗
0.44	2004	<0.01%	<0.01%	<0.01%	✗	✗	✗
0.43	2004	<0.01%	<0.01%	<0.01%	✓	✓	✓
...	2003-2004	<0.01%	<0.01%	<0.01%	✓	✓	✓
0.39	2003	-	-	-	✓	✓	✓
0.38	2003	<0.01%	<0.01%	-	✗	✗	✗
...	2003	<0.01%	<0.01%	<0.01%	✗	✗	✗
0.23	2003	<0.01%	-	-	✗	✗	✗
BitviseSSH:							
9.31	2023	<0.01%	-	<0.01%	✓	✓	✓
9.29	2023	<0.01%	-	<0.01%	✓	✓	✓
8.49	2021	<0.01%	-	<0.01%	✓	✓	✓
7.46	2018	<0.01%	-	<0.01%	✓	✓	✓
6.51	2018	<0.01%	-	<0.01%	✓	✓	✓
WolfSSH:							
1.4.14	2023	<0.01%	<0.01%	<0.01%	✓	✓	✓



Does it work? Yep!

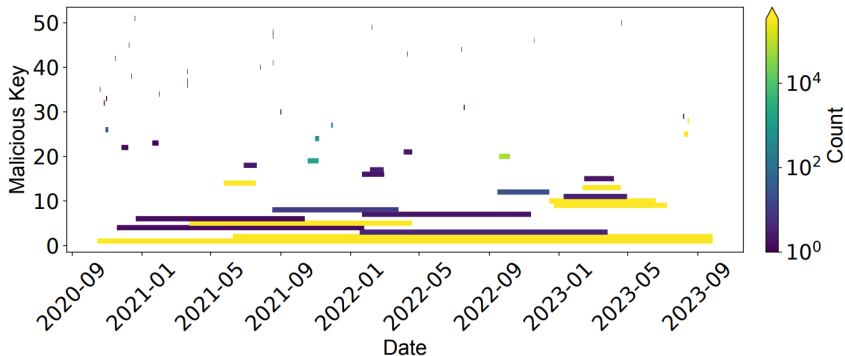


- Implemented as a Zgrab2 module
- Tested on:
 - OpenSSH v9.4-v2.1.1
 - Dropbear v0.84-v0.23
 - BitviseSSH v9-v6
 - WolfSSH v1.4

	Year	Censys (all ports) 2024-04-16	Our Scan (22, 2222) 2024-04-05	Censys (22, 2222) 2024-04-24	Deployment Zgrab	Zgrab2	Pubkey Login
OpenSSH:							
9.4	2024	<0.01%	<0.01%	<0.01%	✓	✓	✓
...	2016-2024	29.21%	22.7%	46.1%	✓	✓	✓
7.4	2016	23.01%	17.00%	18.08%	✓	✓	✓
...	2001-2016	22.28%	12.3%	6.17%	✓	✓	✓
3.0	2001	<0.01%	<0.01%	<0.01%	✓	✓	✓
2.9	2001	<0.01%	<0.01%	<0.01%	✓	✓	✗
...	2000-2001	<0.01%	<0.01%	<0.01%	✓	✓	✗
2.1.1	2000	<0.01%	<0.01%	<0.01%	✓	✓	✗
Dropbear:							
0.84	2024	<0.01%	<0.01%	<0.01%	✓	✓	✓
...	2019-2024	2.42%	0.91%	0.77%	✓	✓	✓
0.78	2019	8.36%	10.01%	12.74%	✓	✓	✓
...	2005-2019	3.51%	1.23%	3.80%	✓	✓	✓
0.47	2005	<0.01%	<0.01%	<0.01%	✓	✓	✓
0.46	2005	<0.01%	<0.01%	<0.01%	✗	✗	✗
...	2004-2005	<0.01%	<0.01%	<0.01%	✗	✗	✗
0.44	2004	<0.01%	<0.01%	<0.01%	✗	✗	✗
0.43	2004	<0.01%	<0.01%	<0.01%	✓	✓	✓
...	2003-2004	<0.01%	<0.01%	<0.01%	✓	✓	✓
0.39	2003	-	-	-	✓	✓	✓
0.38	2003	<0.01%	<0.01%	-	✗	✗	✗
...	2003	<0.01%	<0.01%	<0.01%	✗	✗	✗
0.23	2003	<0.01%	-	-	✗	✗	✗
BitviseSSH:							
9.31	2023	<0.01%	-	<0.01%	✓	✓	✓
9.29	2023	<0.01%	-	<0.01%	✓	✓	✓
8.49	2021	<0.01%	-	<0.01%	✓	✓	✓
7.46	2018	<0.01%	-	<0.01%	✓	✓	✓
6.51	2018	<0.01%	-	<0.01%	✓	✓	✓
WolfSSH:							
1.4.14	2023	<0.01%	<0.01%	<0.01%	✓	✓	✓



Who you gonna... scan for?



Big thanks to: Bitdefender.



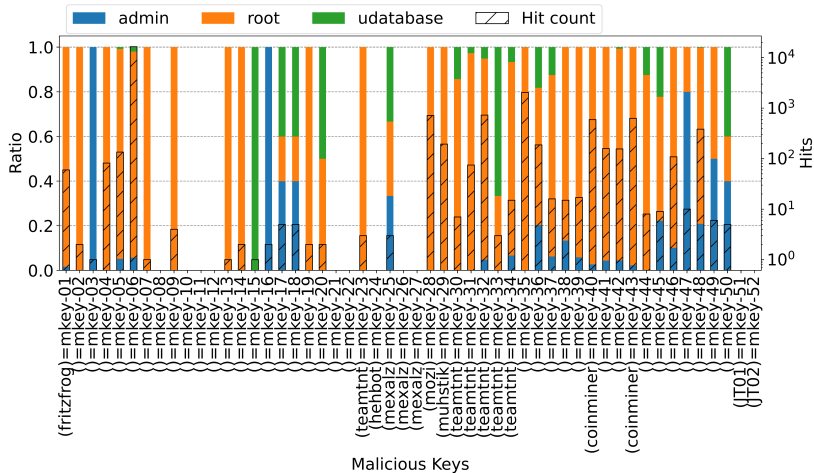
Soooo.... watcha doin? :-)



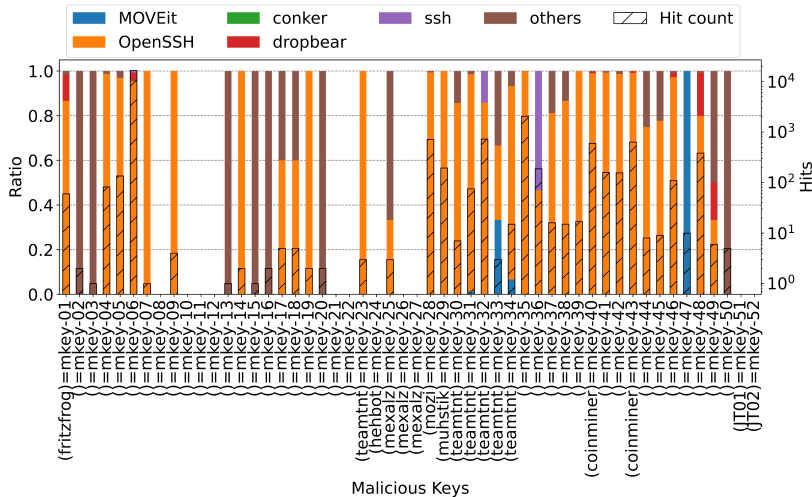
- Scan procedure:
 - We use Zmap for scanning the open ports.
 - We use Zgrab2 to send the payload. (Custom patch to send the MSG_USERAUTH_REQ [user, pubkey])
 - We use a “canary key” (newly generated key) to test the servers before testing actual keys.
 - We actually *read* (and reply to out abuse@)
- What we scan:
 - tcp/22 & tcp/2222
 - Users: ‘root’, ‘admin’, and ‘udatabase’
 - 52 malicious keys (incl. the XZ ones; No, we didn’t find anything)
 - IPv4 & IPv6
 - Still doing it (“The beatings scans will continue until morale security improves.”)



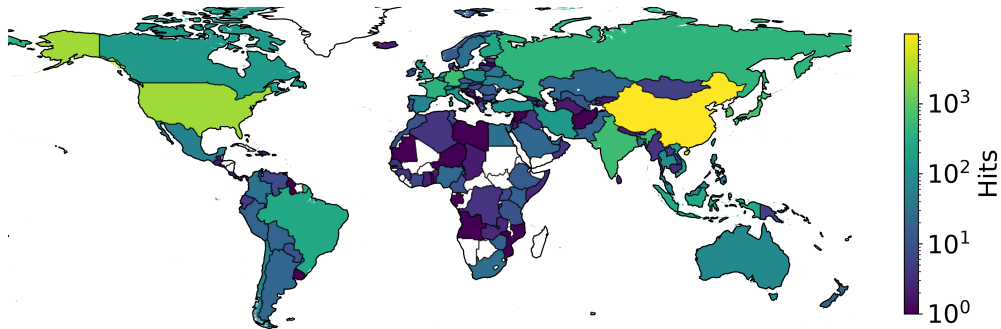
Ca. 21,700 hits in the first scan



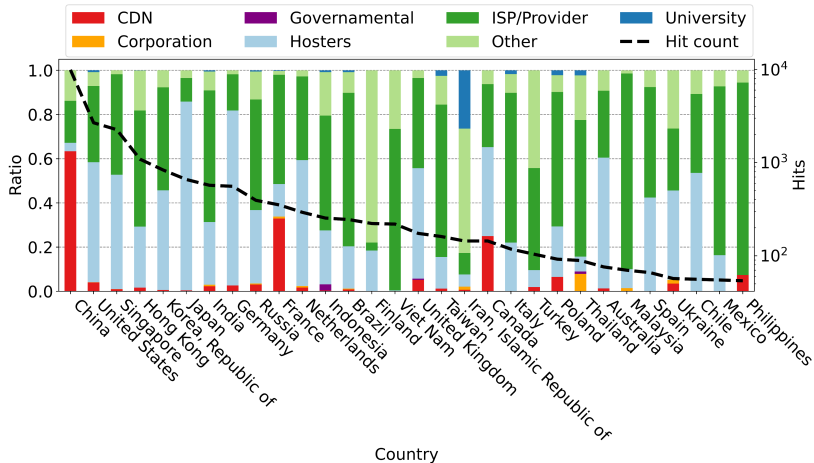
Specialization; So important.



All around the world... *sing*



...orgs do stupid stuff...



Anonymous 'love letters'...



```
Subject:      Re: Abuse from 2a02:d480:4c0:10d4:42::1
Date:        Wed, 13 Dec 2023 16:47:50 +0100
From:        Webmaster <webmaster@...>
To:          Cristian Munteanu <cmuntean@mpi-inf.mpg.de>
CC:          abuse@mpi-klb.mpg.de, INET Scans <inet-scans@mpi-inf.mpg.de>
```

This is not about the "scientific community" is about the law.

You can't scan ports, protocols or addresses, that do not belong to you without a PREVIOUS AND EXPLICIT authorization from the owners.

If you do so, you are involved in criminal activities and we will rise the issue to our lawyer for a criminal case and make it public in social networks.



...are really fun if you know who wrote them.



From: Tobias Fiebig <tfiebig@mpi-inf.mpg.de>
Reply-To: tfiebig@mpi-inf.mpg.de
To: Webmaster <webmaster@>, Cristian Munteanu <cmuntean@mpi-inf.mpg.de>
Cc: abuse@mpi-klsb.mpg.de, INET Scans <inet-scans@mpi-inf.mpg.de>
Subject: Re: Abuse from 2a02:d480:4c0:10d4:42::1
Date: Wed, 13 Dec 2023 20:31:46 +0100

Hello (and/or colleagues),

please allow me to chime into this discussion before it derails even further.



On Wed, 2023-12-13 at 16:47 +0100, Webmaster wrote:

> This is not about the "scientific community" is about the law.



I seem to be getting a 6th sense...



From noc@ [redacted] 
To abuse@mpi-klsb.mpg.de <abuse@mpi-klsb.mpg.de> 
Subject Abuse report - IP address: 2A02:D480:4C0:10D4:42::3

Hi,

We detected a network attack from your network, a computer/VM connected to it is probably infected and being part of a botnet.

Please check it and fix it up as soon as possible.

The following intrusion attempts were detected:

```
May 28 01:26:50.313 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:50.313 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:50.353 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:50.353 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:50.353 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:51.353 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:51.357 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:51.393 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:51.393 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 01:26:51.405 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 02:26:46.064 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 02:26:46.072 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 02:26:46.088 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
May 28 02:26:46.100 CEST: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed]
```



...or...



From: [\[redacted\]@stadtwerke- \[redacted\]](#)
To: [abuse@mpi-klb.mpg.de](#) <[abuse@mpi-klb.mpg.de](#)>
Subject: **Ihr Netzwerk-Scan**

Sehr geehrte Damen und Herren,
wir haben gestern und in den letzten Tagen von Ihnen unautorisierte Anmeldeversuche verzeichnet.
Wir bitten um Mitteilung über den Zweck.

Username: root, admin, udatabase etc.

16 mesz: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed] at 19:00:16 mesz Sun May 26 2024
nw_device_hostname
timestamp
2024-05-26 19:00:17.593

mesz: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 2A02:D480:4C0:10D4:42::3] [localport: 22] [Reason: Login Authentication Failed] at 00:21:57 mesz Wed May 29 2024
nw_device_hostname
timestamp
2024-05-29 00:21:58.170



...did we...



From [redacted]
To abuse@mpi-klb.mpg.de
Subject SSH abuse from 2a02:d480:4c0:10d4:42::3

Your 2a02:d480:4c0:10d4:42::3 host abuses my SSH server (UTC+02:00):

```
May 22 15:30:44 router sshd[5493]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 51870 [preauth]
May 22 15:30:48 router sshd[5496]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 54948 [preauth]
May 22 16:30:40 router sshd[6301]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 58174 [preauth]
May 22 16:30:41 router sshd[6304]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 33334 [preauth]
May 22 17:30:40 router sshd[7021]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 39302 [preauth]
May 22 17:30:41 router sshd[7024]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 56002 [preauth]
May 22 18:30:40 router sshd[7743]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 34470 [preauth]
May 22 18:30:41 router sshd[7746]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 55012 [preauth]
May 22 19:30:41 router sshd[9833]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 51654 [preauth]
May 22 19:30:42 router sshd[9836]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 60074 [preauth]
May 22 20:30:41 router sshd[10903]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 38420 [preauth]
May 22 20:30:41 router sshd[10906]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 38726 [preauth]
May 22 21:30:41 router sshd[11752]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 50048 [preauth]
May 22 21:30:42 router sshd[11755]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 41508 [preauth]
May 23 00:08:07 router sshd[13732]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 41416 [preauth]
May 23 00:08:10 router sshd[13734]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 35556 [preauth]
May 23 01:08:04 router sshd[14476]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 41068 [preauth]
May 23 01:08:04 router sshd[14478]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 40566 [preauth]
May 23 02:08:04 router sshd[15180]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 48496 [preauth]
May 23 02:08:05 router sshd[15183]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 39306 [preauth]
May 23 03:08:04 router sshd[15897]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 57866 [preauth]
May 23 03:08:05 router sshd[15900]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 58488 [preauth]
May 23 04:08:04 router sshd[16684]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 50110 [preauth]
May 23 04:08:05 router sshd[16687]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 32802 [preauth]
May 23 05:08:04 router sshd[17386]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 36362 [preauth]
May 23 05:08:06 router sshd[17389]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 37432 [preauth]
May 23 06:08:03 router sshd[18071]: Connection closed by authenticating user root 2a02:d480:4c0:10d4:42::3 port 44164 [preauth]
```



...miss them for v4?



```
May 30 04:59:25.702: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 04:59:29.025: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 04:59:38.646: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 04:59:41.973: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 05:59:34.965: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 05:59:48.087: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 06:59:29.309: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 06:59:41.204: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 07:59:28.590: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 07:59:31.908: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 07:59:41.839: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 07:59:45.189: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
May 30 08:59:32.378: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: udatabase] [Source: 2A02:D480:4C0:10D4:42::3]
brute force attack from 2A02:D480:4C0:10D4:42::3?
happen to edge01, edge04 and edge05..
can sent to ISP to check
as 680
```



...miss them for v4?



From: [REDACTED]
To: abuse@mpi-klsb.mpg.de <abuse@mpi-klsb.mpg.de>
Cc: [REDACTED] nw core [REDACTED]
Subject: Brute force attack from the Source : 2A02:D480:4C0:10D4:42::3
Date: Fri, 31 May 2024 03:11:12 +0000 (05/31/2024 05:11:12 AM)

Dear AS680,

We did receive a lot logs which trying to access our devise from the below IP.

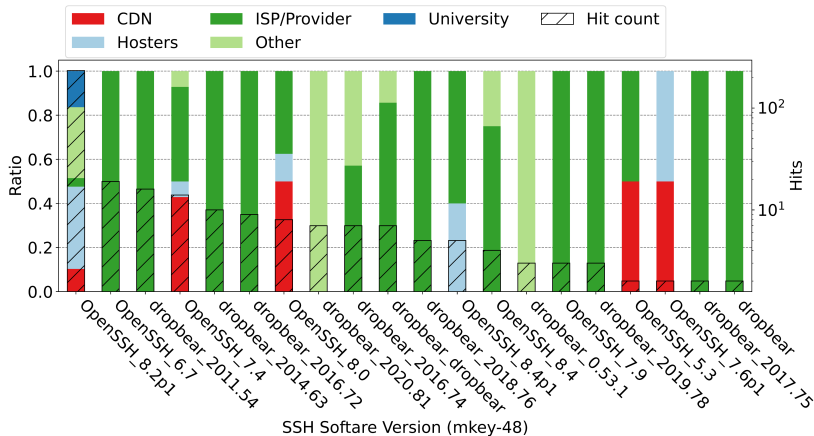
2A02:D480:4C0:10D4:42::3

Here attach the related logs.

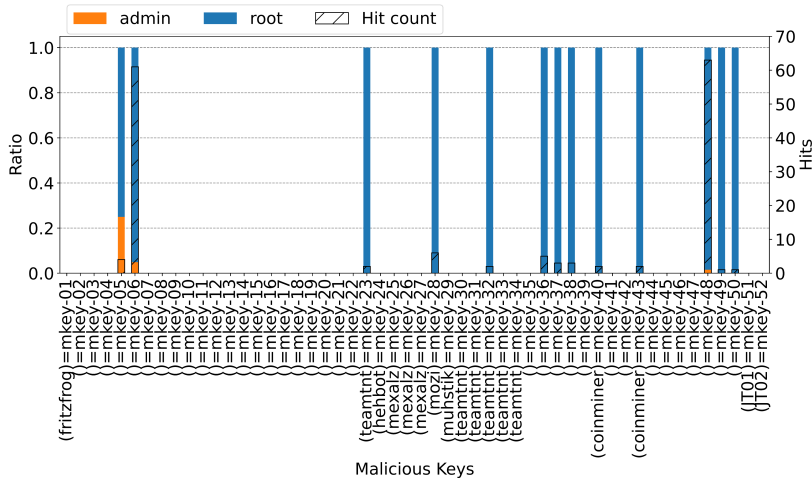
Can you please do assist to fix the situation ?



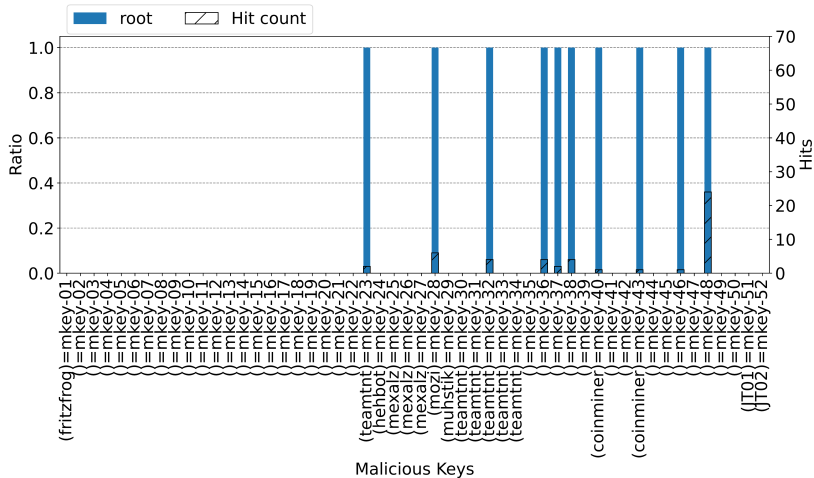
All good things are mkey-48



There and Back(door) again...



... by Hoster Bagging.



Ring me up...



The Shadowserver Foundation

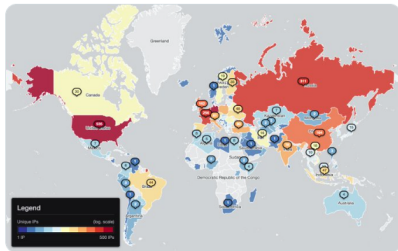
@Shadowserver

...

We are sharing out a Special Report on Compromised SSH hosts detected through leakage of malicious public SSH keys placed on them by attackers: shadowserver.org/what-we-do/net...

3327 compromised hosts detected on IPv4/IPv6 using this methodology.

For background: rushter.com/blog/public-ss...



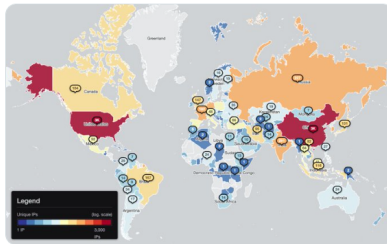
The Shadowserver Foundation

@Shadowserver

...

Heads up! We are sharing out a second Special Report on Compromised SSH hosts detected through leakage of malicious public SSH keys placed on them by attackers: shadowserver.org/what-we-do/net...

This time 10020 compromised hosts found. Top countries US (3K), China (2.9K), Singapore (423)



Now what?

- Subscribe to the Shadowserver feed!
- Clean up your networks! (Yes, seriously)
- Don't write angry 'love letters';
 - we know you only do it when it's not real attackers.
- Some scans are good; You can Opt out...
... but then at least DIY!



The Shadowserver Foundation

@Shadowserver

Heads up! We are sharing out a second Special Report on Compromised SSH hosts detected through leakage of malicious public SSH keys placed on them by attackers: shadowserver.org/what-we-do/net...

This time 10020 compromised hosts found. Top countries US (3K), China (2.9K), Singapore (423)

