State-encouraged BGP hijacking

Marco d'Itri
<md@linux.it>
@rfc1036

End Summer Camp 2K15 - Sep 5, 2015

Background

Hacking Team

A provider of offensive intrusion and surveillance software used by law enforcement and intelligence agencies in many countries.

The 2015 data breach

An unknown entity thoroughly owned Hacking Team and managed to exfiltrate over 400 GB of data, among them the employees' mailboxes, which then have been indexed by Wikileaks.

My analysis

This presentation is based on the content of these emails, whose veridicity has not been challenged, and corroborated by BGP routing data publicly archived by third parties.

Chains of anonymizing proxies

Hacking Team's flagship product is RCS, a malware which uploads the data gathered from the target's computer to a remote server, using a chain of special purpose anonymizing proxies installed on rented servers all over the world.

In august 2013 Santrex, a Russian supplier of some proxy servers used by HT for their customers, had serious technical issues that caused some of these proxies to become unreachable by instances of RCS deployed by the Carabinieri.

A request for BGP hijacking

On 14 august 2013 the Carabinieri sent to *Company X* a request to:

> *[...] publish and then propagate, at least at a national level on the internet network, of the network 46.166.163.0/24.*
>
> *(my translation)*

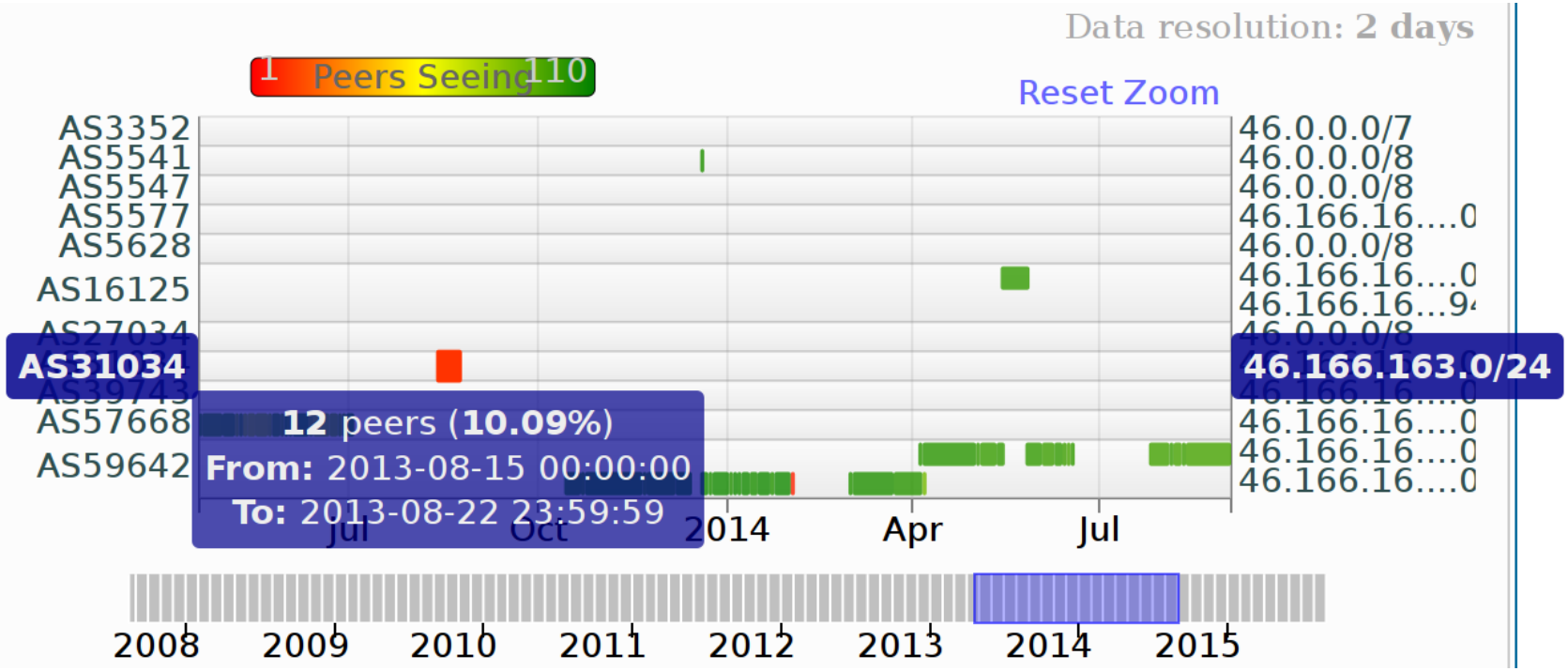
and to make available a server with a specific IP address on this network.

46.166.163.136/29 is a network assigned to Santrex.

It is my understanding that this is a normal request for providing commercial services and not a mandatory order.

Verifying with hard data

Thanks to the awesome RIPEstat service I was able to quickly verify that 46.166.163.0/24 was announced by *Company X* in this period.



The actual scope of this hijacking

Verification

- Downloaded a BGP table dump for 20 august 2013 from the RIPE RIS archive.
- Processed it with my zebra-dump-parser program to extract the routes for 46.166.163.0/24.

Apparently *Company X* advertised the network to all their peers since it was also received e.g. by Hurricane Electric at MIX-IT.

The hijacking was not limited to a couple of local networks: the route was also propagated to others foreign networks.

An unprecedented breach of trust

- *Company X* deliberately announced the IP addresses of a foreign competitor, without their permission, to solve a technical issue of an italian law enforcement agency.
- The hijacked network was propagated all over the world.
- This kind of activity is forbidden by the policies of exchange points, by peering agreements and by transit providers.
- But *Company X* argues that this is totally fine since a LEA asked them do do it.
- As far as I know, this never happened before.

Questions?

`http://www.linux.it/~md/text/state-hijacking.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)

Bonus slide

Independent confirmations of my research:

- BGPmon/OpenDNS
- Renesys/Dyn Research

Articles about the hijacking:

- Ars Technica
- Brian Krebs
- Heise online
- Golem.de
- Engadget
- Wired UK

The emails from the Hacking Team archive:

1 2 3 4 5 6 7 8 9