BGPstream and The Curious Case of AS12389

Posted by Andree Toonk - April 27, 2017 - Hijack - No Comments

The world of BGP routing is a fascinating place with lots of interesting BGP events happening every day. It can be challenging to keep track of it all and so two years ago we started the BGPstream website where we keep track of large scale outages and BGP hijacks. We list the events, basic info and visualize it with one of my favorite tools: BGPlay. For those who keep an eye on @bgpstream , you probably noticed a curious series of BGP hijacks today all by the same Autonomous system affecting many well known networks.

Starting at April 26 22:36 UTC till approximately 22:43 UTC AS12389 (PJSC Rostelecom) started to originate 50 prefixes for numerous other Autonomous systems. The 50 hijacked prefixes included 37 unique autonomous systems and the complete list of affected networks can be found below. If your organization is in this list feel free to reach out and we can provide more details if needed. Keep in mind that many of these hijacks are already published on BGPstream.com as well.

So back to this incident, what happened here? What makes the list of affected networks 'curious' is the high number of financial institutions such as for example: MasterCard,Visa, Fortis,Alfa-Bank,card complete Service Bank and more.

The other curious thing is that this included several more specific prefixes. One example is this one for HSBC https://bgpstream.com/event/80330
This indicates this is not your typical 'leak' (say BGP > OSPF > BGP). Because the prefix normally exist as 203.112.90.0/23 not as the /24 announced by Rostelecom. So someone (likely 12389 Rostelecom) is inserting it in their routing tables themselves. The question is why? One typical scenario where this is normally done is because of some kind of traffic engineering or traffic redirection.

Latest Tweets

Tweets by @bgpmon

BGPmon.net Retweeted

Dan Goodin
@dangoodin001

Russian-controlled telecom hijacks financial services' Internet traffic. Visa, MasterCard, Verisign all affected arstechnica.com/?p=1085633

Russian-controlled tel...
Visa, MasterCard, and Sy...
arstechnica.com

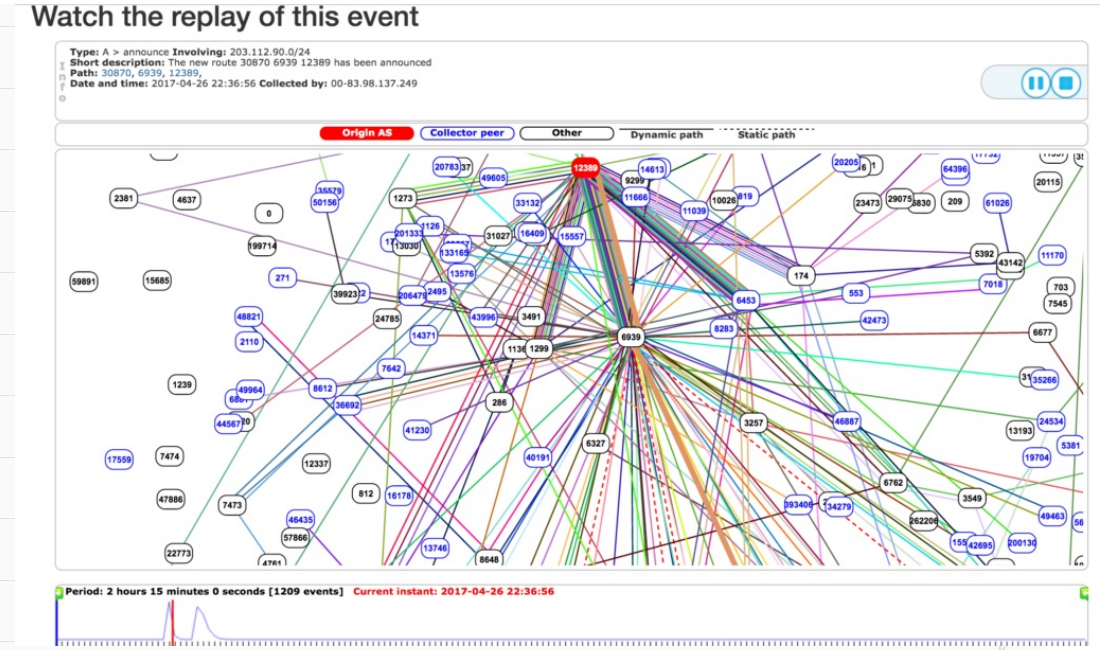
27 Apr

BGPmon.net Retweeted

Ars Technica
@arstechnica

Russian-controlled telecom

Embed View on Twitter



It's also worth noting that at the same time as the hijacks we did see many (78) new advertisements *originated* by 12389 for prefixes by 'other' Rostelecom telecom ASns (29456,21378,13056,13118,8570). So something probably went wrong internally causing Rostelecom to start originating these new prefixes.

Never attribute to malice that which is adequately explained by... well let's say an innocent misconfiguration. If this was in-fact an attempt to on purpose redirect traffic for some of these financial institutions, it was done in a very visible and large scale manner, so from that perspective perhaps not too likely. Then again, given the number of high value prefixes of all the same category (financial institutions and credit card processors) it seems a bit more than an innocent accidental hijack, especially considering the fact that new more specific prefixes were introduced.

For sure an interesting and curious case, so keep an eye on @bgpstream or sign-up for our BGP monitoring service and be alerted as soon as it happens!

Below the list of affected networks (other Rostelecom networks excluded)

AS	Autonomous System Name
49002	Federal State Unitary Enterprise Russian
3561	Savvis
41268	LANTA Ltd
2559	Visa International
8255	Euro-Information-Europeenne de Traitemen
31627	Servicios Para Medios De Pago S.A.
701	MCI Communications Services, Inc. d/b/a
3259	Docapost Bpo SAS
3303	Swisscom (Switzerland) Ltd
3741	IS
5553	State Educational Institution of Higher

5630	Worldline SA
8291	The Federal Guard Service of the Russian
8677	Worldline SA
9162	The State Educational Institution of Hig
9221	HSBC HongKong
9930	TIME dotCom Berhad
11383	Xand Corporation
12257	EMC Corporation
12578	SIA Lattelecom
12954	SIA S.p.A.
15468	38, Teatralnaya st.
15632	JSC Alfa-Bank
15742	PJSC CB PrivatBank
15835	ROSNIIROS Russian Institute for Public N
15919	Servicios de Hosting en Internet S.A.
18101	Reliance Communications Ltd.DAKC MUMBAI
25410	Bank Zachodni WBK S.A.
26380	MasterCard Technologies LLC
28827	Fortis Bank N.V.
30060	VeriSign Infrastructure & Operations
34960	Netcetera AG
35469	Ojsc Bank Avangard
50080	Provus Service Provider SA
50351	card complete Service Bank AG
61100	Norvik Banka AS
200163	Itera Norge AS

No comments

Leave a Reply

Comment

Name

Email

Website

reCAPTCHA

Faça upgrade para um navegador compatível para receber um desafio reCAPTCHA.

Como alternativa, se você acha que a exibição dessa página é um erro, verifique sua conexão à Internet e atualize.

Por que isso está acontecendo comigo?

Privacidade - Termos

Post Comment