THE CURIOUS SILENCE ABOUT THE MOSTLY UNREMARKED RUSSIAN BGP HIJACK

These days, it seems that NYT-approved columnists and self-appointed THREADsters can start a conspiracy theory about anything just by slapping the label “Russia” on it. Which is why I find it so curious that the BGP hijack last week of a bunch of finance companies (and some other interesting targets) by Russian telecom Rostelecom has gone generally unnoticed, except by Ars’ Dan Goodin.

Here’s a great description of what the Border Gateway Protocol is — and why it’s ripe for hijacking.

> Such is the story of the “three-napkins protocol,” more formally known as Border Gateway Protocol, or BGP.
>
> At its most basic level, BGP helps routers decide how to send giant flows of data across the vast mesh of connections that make up the Internet. With infinite numbers of possible paths — some slow and meandering, others quick and direct — BGP gives routers the information they need to pick one, even though there is no overall map of the Internet and no authority charged with directing its traffic.
>
> The creation of BGP, which relies on individual networks continuously sharing information about available data links, helped the Internet continue its growth into a worldwide network. But BGP also allows huge swaths of data to be “hijacked” by almost anyone with the necessary skills and access.
>
> The main reason is that BGP, like many

> key systems on the Internet, is built to automatically trust users — something that may work on smaller networks but leaves a global one ripe for attack.

As BGPstream first noted, the data streams for 37 entities were rerouted by Rostelecom manually last Wednesday for a 6 minute period.

> 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

The victims include Visa, Mastercard, Verisign, and Symantec.

Oh — and according to BGPmon, the victims also include Alfa bank — the bank that got mentioned in Christopher Steele's dossier, that had some weird behavior involving a Trump marketing server last summer, and one of two banks for which the FBI allegedly got a FISA order as part of the investigation into Russia's interference in the US election.

BGPmon provides one possible innocent explanation (which is, in fact, the analogue of the innocent explanation offered for the Alfa-Trump traffic): it could be BGP advertising gone wrong.

> 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.

But Goodin provides some reasons why the hijack should be treated with suspicion. First, Rostelcom – the company that hijacked this traffic – is considered an official Russian government entity.

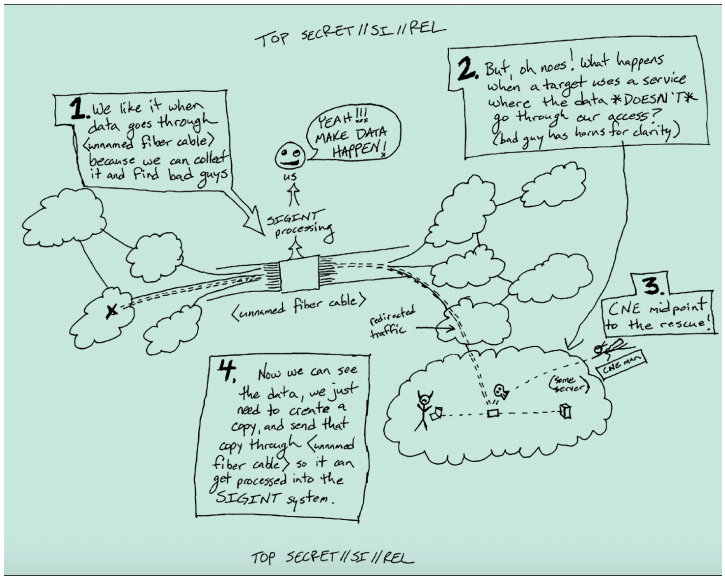
> According to shareholder information provided by Rostelecom, the Russian government owns 49 percent of the telecom's ordinary shares. The US Department of Commerce lists Rostelecom as a state-owned enterprise and reports that one or more senior government officials have seats on Rostelecom's board of directors. Rostelecom officials didn't respond to e-mail seeking comment for this post.

He cites Dyn's Doug Madory explaining why the targeted nature of this hijack should rouse suspicion.

> "I would classify this as quite suspicious," Doug Madory, director of Internet analysis at network management firm Dyn, told Ars. "Typically accidental leaks appear more voluminous and indiscriminate. This would appear to

> be targeted to financial institutions. A typical cause of these errors [is] in some sort of internal traffic engineering, but it would seem strange that someone would limit their traffic engineering to mostly financial networks."

As Goodin notes, and as I have before, one reason an entity (especially a government) might want to hijack traffic is to make it cross a router where it has the ability to collect it for spying purposes. That process was described in some presentations from an NSA hacker that the Intercept published last year.



As Goodin notes, given that the victims here should be presumed to be using the best encryption, it would take some work for Rostelecom to obtain the financial and other data in the traffic it hijacked.

> Such interception or manipulation would be most easily done to data that wasn't encrypted, but even in cases when it was encrypted, traffic might still be decrypted using attacks with names such as Logjam and DROWN, which work against outdated transport layer security implementations that some organizations still use.
>
> Madory said that even if data couldn't

> be decrypted, attackers could potentially use the diverted traffic to enumerate what parties were initiating connections to MasterCard and the other affected companies. The attacker could then target those parties, which may have weaker defenses.

But there's at least one other reason someone might hijack traffic. If you were able to pull traffic off of switches you knew to be accessible to an adversary that was spying on you, you might succeed in detasking that spying, even if only for 6 minutes.

One of my all-time favorite Snowden disclosures revealed that the NSA was forced to detask from some IRGC Yahoo accounts because they were being spammed and the data was flooding NSA's systems. That happened at precisely the moment that the FBI was trying to catch some IRGC figures in trying to assassinate then Saudi Ambassador to the US (and current Foreign Secretary) Adel al-Jubeir, which I find to be a mighty interesting coinkydink.

This hypothetically could be something similar: a very well-timed effort to thwart surveillance by making it inaccessible to the switches from which the NSA was collecting it (though honestly, it would take some doing to pull traffic off all collection points accessible to the NSA, and I'm not even sure that would be possible for transatlantic traffic).

Don't get me wrong. Accidental or not, this was a foot-stomping event. I'm sure the competent and responsible authorities at both the victim companies and the NSA *have* taken notice of this event, and are working to understand why it happened and if anything was compromised by it.

But I find it striking that the thousands of people spending all their time fervently creating conspiracies where none exist have not even noticed this event which, whatever it explains it, was a real event, and one

involving the bank that has been at the center of so many real and imagined conspiracies.