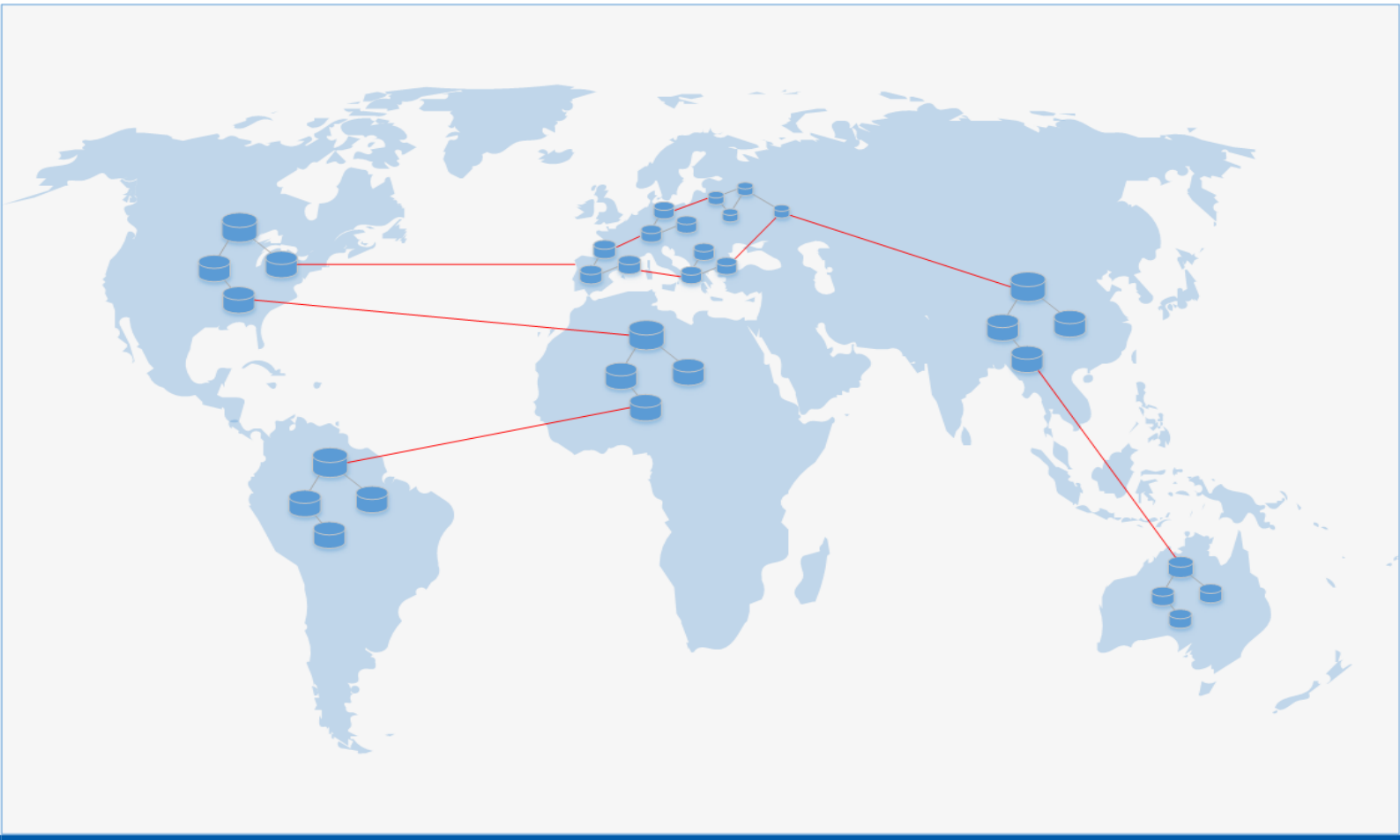
enisa

THE EU CYBERSECURITY AGENCY



7 STEPS TO SHORE UP BGP

MAY 2019

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For technical queries about this paper, please email resilience@enisa.europa.eu
For media enquires about this paper, please email press@enisa.europa.eu.

AUTHORS

Aggelos Koukounas, Eleni Vytogianni, Marnix Dekker

ACKNOWLEDGEMENTS

We would like to thank Ilias Bakatsis (until recently working at ENISA), and Andrei Robachevsky, a subject matter expert (CEI) contracted by ENISA, for their work on the preliminary analysis of BGP security. We are grateful to the 63 EU telecom providers who participated in the 2018 ENISA BGP Security survey. We thank the ETIS INFOSEC WG for the collaboration and input received through them. We are grateful for the useful comments and feedback received from Rolv Hauge (Telenor), Stefano De Crescenzo and colleagues (CISCO), Alejandro Becerra Gonzalez and colleagues (Telefonica), Stefan Pütz and colleagues (Deutsche Telekom). This paper was reviewed by the ENISA Article 13a Expert Group, comprising of national telecom regulatory authorities (NRAs) from across Europe.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-294-3 DOI: 10.2824/66344

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BGP, the Border Gateway Protocol, is a central part of the internet backbone. It is used by internet service providers to relay internet traffic across the globe. It was designed more than 25 years ago and when it was introduced the main requirement was resilience, simplicity, and ease of deployment. BGP lacks security which make it vulnerable to attacks and misconfiguration errors.

Famously in 2008 an ISP in Pakistan, in an effort to censor a Youtube video, diverted the whole world's Youtube traffic to Pakistan, effectively making the website unavailable for everyone. Recently we have seen more and more attacks exploiting the weaknesses in BGP.

- In 2017, 80 prefixes for high profile destinations (Google, Apple, Facebook, Microsoft, etc), were being announced by a previously unused Russian Autonomous System (AS), affectively rerouting this traffic through Russia[1].
- In 2018, a BGP hijack was used to divert internet traffic to the Amazon EC2 cloud, with the goal of stealing Ethereum crypto-currency.
- In 2018, a BGP hijack was used to divert traffic to Google from subscribers living in the west of the USA, via Russia, to China, allegedly intentionally and for espionage purposes[2].

There are many more BGP attacks and BGP misconfigurations which do not make the headlines. Many BGP hijacks even go unnoticed because they are not easily noticed by the end-users because there is no outage.

BGP attacks can be used for many different purposes, ranging from financial crime targeting a few users (for stealing crypto currency) to large scale espionage and disruption. If unmitigated, the security vulnerabilities of BGP lead to risks of large scale network outages, impacting the economy and society, privacy risks for citizens, risks for companies, risks for national security, risks of espionage, etc. These risks are increasing, because there is an increase in the number and sophistication of cyber-attacks, on the hand, and on the other hand an increased reliance on the internet.

In 2018 ENISA conducted a survey to assess the state of play of BGP security in Europe. Our survey collected 63 responses from large and small electronic communication providers across the EU. Our survey showed that BGP hijacks are common and that these incidents have a high impact: 44 percent of providers answering the survey said that the impact of BGP incidents is high, affecting large numbers of users and lasting for many hours.

In this paper we highlight the security vulnerabilities of BGP and explain why it is so important to address them. Working closely with experts from industry we derived a shortlist of 7 basic BGP security measures which are industry good practices that should be relatively simple to adopt and relatively effective. We encourage electronic communications providers and other organizations running an Autonomous System (AS) to implement these 7 measures as a minimum.

Our survey showed that BGP hijacks are common and that these incidents have a high impact: 44 percent of providers answering the survey said that the impact of BGP incidents is high, affecting large numbers of users and lasting for many hours.

[1] https://bgpmon.net/popular-destinations-rerouted-to-russia/
[2] https://www.theregister.co.uk/2018/11/13/google_russia_routing/

- **BGP Monitoring and Detection**: Monitor internet traffic routes for your internet traffic, to detect anomalies, not only to guarantee resilience but also for the privacy and security of subscribers.
- **BGP Coordination**: It is crucial to coordinate with peers, by publishing route policies and partaking in peering databases.
- **Prefix Filtering**: It is important to filter prefixes that should never be announced or forwarded in your network, both on ingress and egress network traffic.
- **BGP AS Path Filtering**: It is important to filter BGP AS path attributes for items that should not be allowed in BGP route announcements to into or out of your network.
- **Bogon Filtering**: It is important to filter out bogus prefixes (also called bogons), as these prefixes should never appear in BGP announcements.
- **TTL Security (GTSM)**: It is important to implement TTL security, which makes it harder attack BGP sessions.
- **RPKI**: It is important to implement RPKI and digitally sign route announcements to allow peers to check that announcements are authentic and authorized.

In Section 3, we explain these BGP security measures in more detail. In the annex of this paper, we include checklist for these measures.

This work on BGP security was done in the context of Article 13a of the Framework directive, which asks EU Member States to ensure that providers take appropriate security measures to protect their networks and services. For the last decade, ENISA has collaborated closely with the EU Member States and experts from national telecom regulatory authorities (NRAs) which supervise this part of the EU legislation, under the ENISA Article 13a Expert Group[3]. The ENISA Article 13a Expert group meets 3 times per year to discuss and exchange information about security in the electronic communications sector.

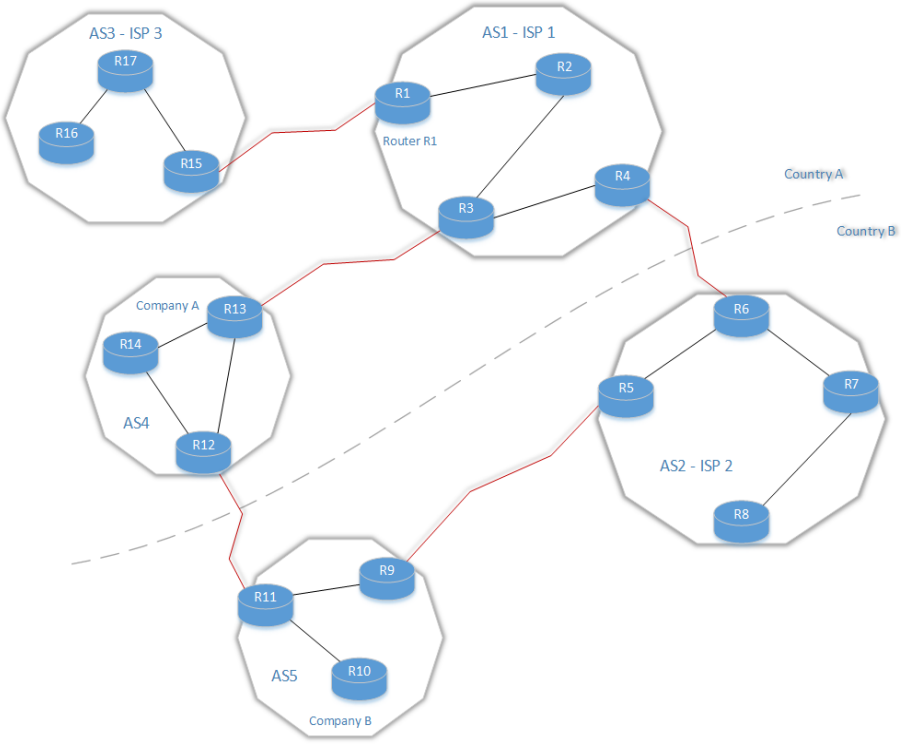
We are grateful for the good collaboration with the NRAs. We also worked closely with security experts from the telecom sector. We are grateful for the valuable contributions from them on this topic.

[3] https://resilience.enisa.europa.eu/article-13

1. INTRODUCTION TO BGP SECURITY

The Border Gateway Protocol (BGP) is a central part of the internet backbone. BGP is an internet interconnection protocol which allows organizations to connect their network, called Autonomous System (AS), to the rest of the internet, allowing them to relay traffic across the globe to the right destination (see the diagram below). Typically ASs are managed by internet service providers, network operators, telecom providers, but there are many other organizations who operate an AS[4]. Every AS implements BGP to exchange routing and reachability information with peer ASs. Basically each AS handles a table with known routes to peer networks and provides this information to peers using IP prefix announcements. The attributes in these announcements, like local preferences, origin, path length, allow each AS to make a local decision about where to route packets.

BGP has some fundamental security weaknesses, which makes it particularly vulnerable to attacks by malicious actors, as well as misconfigurations and errors.



BGP was designed decades ago with interoperability and ease of deployment in mind. BGP has some fundamental security weaknesses, which makes it particularly vulnerable to attacks by malicious actors, as well as misconfigurations and errors.

1.1 PAST BGP INCIDENTS AND ATTACKS

Below we list a number of high-profile BGP incidents reported in the media. Note that not all these incidents are attacks. It is not always easy to distinguish a BGP mistake from a deliberate BGP hijack.

- **Youtube, Pakistan, 2008**: The problems and vulnerabilities of BGP gained widespread attention in 2008 when an ISP in Pakistan, in an effort to censor a Youtube video,

[4] There are more than 60.000 Autonomous Systems. Each AS has a number. AS numbers are assigned in blocks by IANA to regional Internet registries (RIRs). https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html

diverted the whole world's Youtube traffic to Pakistan, effectively making the website unavailable for everyone. What happened technically is that Pakistan Telecom started an unauthorised announcement of a prefix for Youtube, which was by mistake forwarded to the rest of the world by its upstream provider PCCW Global. Youtube was unavailable for everyone for two hours in February 2008[5].

- **China telecom BGP hijack, 2010**: In 2010 China Telecom 'originated' 37000 prefixes (instead of its ususal 40 prefixes) including popular websites like CNN and Amazon[6].
- **Stealing cryptocurrency via BGP exploit, 2014**: In 2014 attackers hijacked a portion of online traffic from a set of 19 ISPs, with the goal of stealing cryptocurrency from a group of users[7].
- **Rostelecom, 2017**: In April 2017 Rostelecom, a Russian ISP, leaked dozens of routes pertaining to IP addresses that belong to major financial services firms. The Russian ISP 'originated' 137 prefixes, 37 of which belong to financial, e-commerce and payment services, like Mastercard, Visa, Forti, Alfabank, etc For 7 minutes, global traffic to these services was redirected via the Rostelecom network[8].
- **Inactive AS in Russia hijacks high profile sites, 2017**: In December 2017, an Autonomous System in Russia, which had been inactive for many years, announced 80 prefixes for high profile domains such as Google, Apple, Facebook, Microsoft, and others[9].
- **Hackers emptying Ethereum wallets, 2018**: In April 2018, attackers intercepted and altered DNS requests for myetherwall.com allowing them to empty Ethereum cryptocurrency wallets. The attack on DNS was achieved via BGP hijacking[10].
- **China telecom BGP hijacks via Russia, 2018**: In 2018 China Telecom established peering points in strategic places around the world, including the US, and then proceeded to hijack traffic using BGP. Recent examples of targeted websites include Google GSuite and Google Search. In November 2018 traffic to Google Analytics was hijacked and redirected to China via Russia.
- **China Telecom BGP hijack of US dpt of Energy, 2019**: In January 2019 China Telecom hijacked 192.208.18.0/23 for 2 hours, which is a prefix belonging to the US Department of Energy[11].

NOT ALL BGP ATTACKS AND INCIDENTS ARE REPORTED INTO MEDIA OR COVERED IN THE NEWS.

1.2 STATISTICS ABOUT BGP ATTACKS

Not all BGP attacks and incidents are reported into media or covered in the news. The Internet Society published a report[12] in 2017, based on data from BGPstream, showing that every year there are thousands such attacks. We citing some of the statistics for 2017.

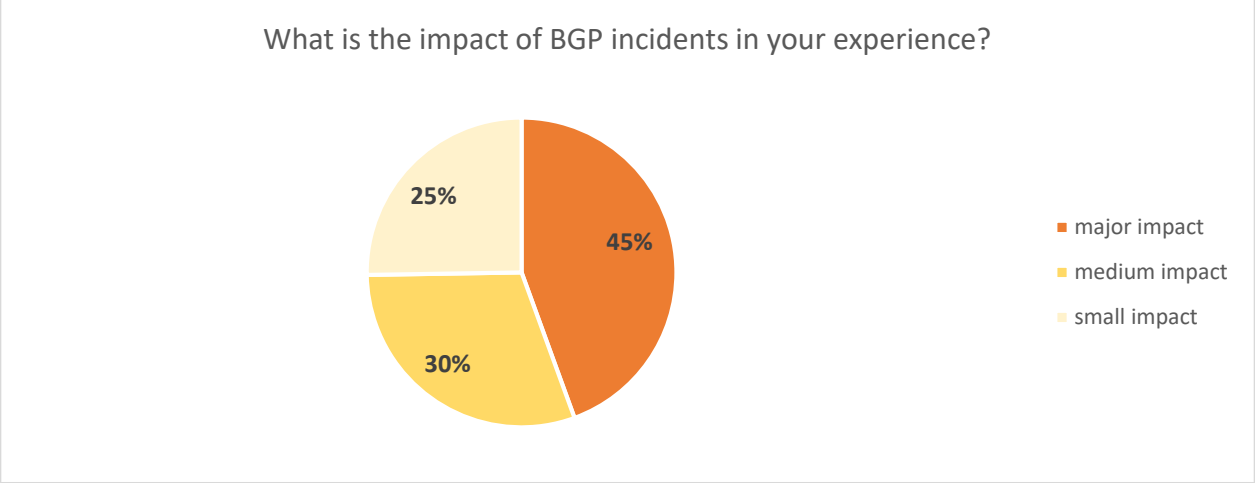
- In 2017 there were almost 14000 BGP incident incidents (either outages or attacks, like route leaks and hijacks).
- Around 3000 Autonomous Systems experienced BGP incidents, i.e. 10% of all Autonomous Systems (at the time) experienced one or more routing incidents.

[5] https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study
[6] https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/
[7] https://www.wired.com/2014/08/isp-bitcoin-theft/
[8] https://blog.thousandeyes.com/rostelecom-route-leak-targets-ecommerce-services/
[9] https://bgpmon.net/popular-destinations-rerouted-to-russia/
[10] https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum
[11] https://bgpstream.com/event/171779
[12] 14,000 Incidents: A 2017 Routing Security Year in Review, https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

1.3 ENISA BGP SECURITY SURVEY 2018

In 2018, ENISA conducted a survey across the EU's electronic communications sector, to get an up to date picture of the situation in Europe. The ENISA survey covered a broad spectrum from European providers, including domestic ISPs but also large international operators and gathered responses from 63 different organizations. The responses underline the seriousness of BGP incidents.

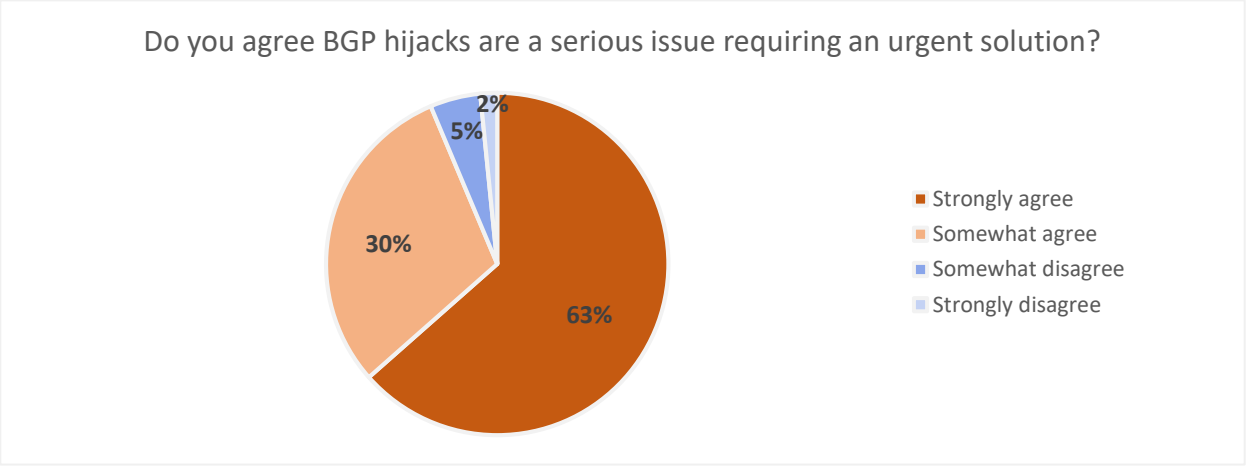
We asked providers to assess the severity of the impact of BGP incidents. Almost half (44%) of the providers experienced incidents with a *"major impact*" on their networks, i.e. long lasting outages affecting many subscribers. A third of the respondents experienced incidents with medium impact (long lasting, affecting few subscribers, or many subscribers short lasting). See the chart below.



The responses to our survey show that there are differences across the EU in terms of what BGP security measures are in place. Some providers *are* implementing industry good practices to mitigate the BGP security vulnerabilities. At the same time certain basic BGP security measures are not in place across the board.

The responses show that while some providers are rarely experiencing BGP security incidents, others see BGP security incidents regularly.

The survey respondents were clear about the urgency of addressing BGP security. Almost two-thirds of the respondents strongly agreed that BGP hijacks are a serious issue, requiring an urgent solution. See chart below.



2. BORDER GATEWAY PROTOCOL SECURITY VULNERABILITIES AND RISKS

In this section we explain the technical security vulnerabilities of BGP and the associated security risks.

2.1 BGP SECURITY VULNERABILITIES

BGP vulnerabilities have been known for a long time already. They are documented for instance in IETF's RFC 4272 "BGP Security Vulnerabilities Analysis", which was published in 2006. BGP has three fundamental vulnerabilities[13]:

1. BGP has no mechanism to protect integrity and authenticity of messages in peer-peer BGP communications.
2. BGP has no mechanism to validate the authority of an AS to announce prefixes or relay route information.
3. BGP has no mechanism to validate the authenticity of the path attributes in prefix announcements.

POSSIBLE ATTACKS ON BGP

- Altering valid BGP peer-to-peer communications
- BGP misorigination aka BGP hijacking
- BGP path attribute tampering
- BGP Policy attacks and route leaks

2.2 POSSIBLE ATTACKS ON BGP

We explain how these security vulnerabilities can be exploited by an adversary. Note that we use the term "adversary" in a lose sense here, because sometimes incidents are the result of unintentional mistakes.

- **Altering valid BGP peer-to-peer communications**: BGP uses TCP/IP for the information exchange between two peers. Long-standing TCP/IP connections, such as BGP sessions, are vulnerable to tampering. An adversary can try to inject BGP messages into the TCP/IP communication between BGP peers, injecting bogus routing information. An adversary can break the connection by inserting spoofed packets. The result of this attack is altering or disrupting the originally valid peer-to-peer communications between BGP peers. This attack can be used to intercept, alter or disrupt internet traffic.
- **BGP misorigination aka BGP hijacking**: BGP mis-origination, also known as BGP hijacking, is when an adversary claims to be the origin of prefixes of another network. If route information is accepted by peers and/or propagated then the "roadmap" of the Internet is altered. The result of this attack is that the traffic is forwarded to the wrong AS. From there the AS could still forward it to the right destination to avoid drawing attention. This attack can be used to intercept, alter or disrupt internet traffic.
- **BGP path attribute tampering**: The BGP path attribute lists which ASs have forwarded a BGP route announcement. The path attribute lists AS numbers (ASNs) in reverse order. The primary purpose of the path attribute is to prevent loops during inter-AS routing. The path attribute is not protected in BGP and any AS which sees the announcement can change it, meaning that an AS cannot be sure that the BGP announcement traversed the networks as indicated.
- **BGP Policy attacks and route leaks**: BGP route announcements have a specific scope, a 'policy', defining where the announcement should be used. The scope of a BGP announcement is usually defined by a set of local redistribution or filtering policies

[13] RFC 4272 "BGP Security Vulnerabilities Analysis", https://datatracker.ietf.org/doc/rfc4272

distributed among the ASs involved. Often, these intended policies are defined in terms of the pair-wise peering business relationship between ASs (e.g., customer, transit provider, peer, upstream). An example of a BGP policy violation is a so-called route leak, i.e. the propagation of a routing announcement beyond their intended scope, in violation of the BGP policies of the receiver, the sender, and/or one of the ASs along the preceding AS path. An adversary can use route leaks to deliberately inject himself in the routing path between outside networks and specific destinations, with relative ease and raising little suspicion. The Pakistan BGP hijack was an example of such a mistake. A route leak can be used to hijack, alter, and disrupt internet traffic.

2.3 BGP SECURITY RISKS

The BGP vulnerabilities can be used in many different ways, from eavesdropping the traffic and silently passing the data forward without disrupting it, to causing internet connection outages which impact the availability of the network. BGP vulnerabilities can also be used to attack weaknesses in other protocols like DNS hijacks. We distinguish 4 main security risks caused by BGP security vulnerabilities:

- **Eavesdropping internet traffic content**: If the internet traffic is unencrypted, BGP attacks can be used to eavesdrop on the content of internet traffic. This can have severe consequences for subscribers, the endpoints, as well as organization on the server-side. The impact for subscribers can include financial impact, stealing of credentials and passwords, privacy issues, etc. If carried out carefully, subscribers will not immediately notice an attack is going on.
- **Altering internet traffic content:** If the internet traffic is unencrypted, BGP attacks can be used to alter internet traffic, for example redirecting subscribers to spoofed websites, tampering with SSL/TLS certificates, altering DNS responses, etc. This can have severe consequences for subscribers. A good example is the recent theft of crypto currency by hijacking internet traffic to the Amazon's EC2 cloud. If carried out carefully, subscribers will not immediately notice an attack is going on.
- **Internet traffic analysis and metadata analysis:** If the internet traffic is encrypted, for instance with SSL/TLS, which is increasingly common, BGP attacks can still be used to intercept so-called traffic metadata, i.e. information about which PCs make connections, to which domains and IPs, from where, to which domains, when, etc. This can be useful for surveillance and espionage. Capturing, even briefly, a swath of the internet traffic will give the adversary precious information about the kind of applications people are using on their PCs, smartphones, the kind of websites they are visiting, from where, when, etc. If carried out carefully, subscribers will not immediately notice that an attack is going on.
- **Internet connection outages:** Internet traffic can be disrupted using BGP attacks. It is relatively easy to cause large-scale disruptions. Such attacks are obviously visible. At the same time, considering the dependency of modern society on internet access, disruptions can have severe economic and societal impact.

These risks lead to risks of large-scale societal and economic disruption (via network outages), privacy risks for citizens using the internet (via eavesdropping of internet traffic metadata or content), risks for national security (via espionage), and so on.

These risks, depending on the setting and the goals of the attacker, in turn lead to risks of large-scale societal and economic disruption (via network outages), privacy risks for citizens using the internet (via eavesdropping of internet traffic metadata or content), risks for national security (via espionage), and so on.

Sidenote about internet traffic encryption with TLS: *Luckily SSL/TLS is becoming more and more widespread and a large part of HTTP traffic now runs over TLS/SSL[14]. Browsers even*

[14] https://transparencyreport.google.com/https/overview?hl=en

warn when a website is not HTTPS. Of course SSL/TLS would mitigate the risks 1 and 2 in the list above. It is important to note that, some websites and domains are still not using TLS[15]. Even if this was not the case there is a lot of other internet traffic that remains unencrypted, such as for instance DNS requests. There are also weaknesses in the global certificate system of CAs called PKI that is used for TLS. This year, 2019, started with a series of DNS hijacks used to create fake TLS/SSL certificates via LetsEncrypt[16] for instance. Experts have argued that the metadata is sometimes more telling than the actual content of communications. Finally it should be said that experts have argued that in many settings the communications metadata can be more revealing than the actual content of communications.[17] SSL/TLS does not hide which clients are connecting to which websites, domains and applications.

[15] https://blog.avira.com/20-of-the-world-502-largest-websites-do-not-use-https/
[16] https://arstechnica.com/information-technology/2019/01/a-dns-hijacking-wave-is-targeting-companies-at-an-almost-unprecedented-scale/
[17] https://www.idgconnect.com/idgconnect/opinion/1012872/metadata

3. BASIC BGP SECURITY MEASURES

BGP security vulnerabilities are a high risk for Europe's internet backbone. Without mitigating measures, attacking BGP is an easy way for an adversary to eavesdrop, intercept or disrupt Europe's internet traffic. Attacks on BGP can cause a major impact, on the privacy of European citizens, on the national security of EU countries, and disrupt society and economy. These BGP attacks are not hypothetical as shown by some recent large scale BGP hijacks.

Below we shortlist 7 basic BGP security measures which are relatively easy to implement and relatively effective in mitigating BGP hijacks. We deliberately kept this list short and focused on the basics, consulting closely with the technical experts from several providers about costs, complexity and effectiveness.

	BGP SECURITY MEASURE	EXPLANATION AND REFERENCES
1	**BGP Monitoring and Detection**	Electronic communications providers, and other organizations running ASs, should monitor and detect routing anomalies which is fundamental to understand the frequency and impact of BGP attacks aiming at the health of the network. They should monitor the global routing of their traffic in order to assess not only stability and resilience, but also privacy and security of their subscribers.
2	**BGP Coordination**	Electronic communications providers, and other organizations running ASs, should make contact data globally accessible and make their routing policies publicly available in IRRs to coordinate with peers. They latter should publish their contact information and publish their routing policies (using Routing Policy Specification Language - RPSL[18]) in IRRs and databases, such as PeeringDB[19], RIPE[20] and RADb[21].
3	**Prefix Filtering**	Electronic communications providers, and other organizations running ASs, should control the prefixes received and advertised. Prefixes in inbound and outbound advertisements should be filtered using IP prefix lists, which is an easy to use mechanism that allows operators to control ingress and egress traffic, from and to customers, peers and upstream providers. Prefix filtering is described in detail in RFC 7454[22] document about 'BGP Operations and Security'.
4	**BGP AS Path Filtering**	Electronic communications providers, and other organizations running ASs, should use BGP AS Path filtering. Path filtering is a technique network administrators can use to permit or deny prefixes from certain autonomous systems. Network administrators can specify different cases in which they should accept or reject prefixes with particular features in the AS path (i.e. prefixes with private AS numbers in the AS path unless the prefixes are from customers). AS-PATH filtering should be applied to customers, peers and upstream providers. AS-PATH filtering is described in detail in RFC 7454[23] document about 'BGP Operations and Security'.
5	**Bogon Filtering**	Electronic communications providers, and other organizations running ASs, should filter bogus prefixes, also known as bogons, which should never appear in the Internet routing table. Some of the prefixes which should be blocked are:

[18] http://www.irr.net/docs/rpsl.html
[19] https://docs.peeringdb.com/
[20] https://www.ripe.net/
[21] https://www.radb.net/
[22] https://tools.ietf.org/html/rfc7454#section-6
[23] https://tools.ietf.org/html/rfc7454#section-9

		1. IP prefixes allowed for public use that are unallocated and have not been assigned to a Regional Internet Registry (RIR) by Internet Assigned Numbers Authority (IANA). 2. IP prefixes used for private use and IP addresses used for loopbacks 3. RIR-allocated IP space that has not been assigned to an ISP or an end-user. It is worth noting that bogon lists are not static lists and should be kept updated. To support static router configuration, which can be difficult, a possible solution is the *Bogon Route Server Project*[24] developed by TEAM CYMRU.
6	**TTL Security (GTSM)**	Electronic communications providers, and other organizations running ASs, should implement TTK Security, which is a lightweight security mechanism used to make BGP sessions harder to spoof. It is based on a value that the BGP receiver should check if it matches with the expected one, during the BGP session. BGP sessions should set their values to 255 and check to ensure that their adjacent BGP session packets have the same value. The mechanism should be implemented on directly-connected BGP peerings. TTL Security (GTSM) is described in detail in RFC 5082[25] document about 'BGP Operations and Security'.
7	**RPKI**	Electronic communications providers, and other organizations running ASs, should implement RPKI. RPKI adds authentication to the routing system using digital signatures. With RPKI providers can sign the prefix containing the origin AS they intend to use, generating in this way a Route Origin Authorization (ROA). Using ROAs for the address space they hold, providers can create cryptographically verifiable statements about their routing intent.

It is important to underline that this is a shortlist and not a complete guide on BGP security, with all measures and good practices. We encourage organization to follow and take into account other industry good practices and initiatives on BGP. We would like to mention some of them:

- MANRS, Mutually Agreed Norms for Routing Security, is a global industry initiative, supported by the Internet Society, to implement crucial fixes needed to reduce the most common routing threats[26].
- BGPsec, specified in IETF RFC 8205, is an extension of the Border Gateway Protocol, designed to assure the authenticity of the AS path, by using digital signatures from each AS propagating announcements[27].
- RIPE NCR recently issued a policy proposal that classifies BGP route leaks are a policy violation[28].

The global internet infrastructure, the backbone, the interconnections, the routing, the domain name system, but also the mobile network infrastructure, has evolved over time. It uses many legacy protocols, designed in the past, often vulnerable to attacks. The problem of vulnerabilities in legacy protocols is a problem that requires continuous attention and effort by providers. SS7 is another example of a legacy interconnection protocol with serious issues[29]. It is crucial that providers keep up to date with good practices in the industry in this regard.

We recommend NRAs across Europe to enquire about the above-mentioned BGP security measures with electronic communication providers and other organisations running an AS, in their constituency. In the annex we provide a basic checklist they can use to collect information.

[24] http://www.team-cymru.com/bogon-reference-bgp.html
[25] https://tools.ietf.org/html/rfc5082
[26] https://www.manrs.org/
[27] https://tools.ietf.org/html/rfc8205
[28] https://www.ripe.net/participate/policies/proposals/2019-03
[29] https://www.enisa.europa.eu/news/enisa-news/legacy-technologies-as-a-threat-to-eu2019s-telecommunications-infrastructure

We would like to thank the NRAs for their collaboration with us and we are particularly grateful for the technical experts from providers from across the EU who have been forthcoming and open about this cross-cutting cybersecurity issue. We look forward to collaborating with them in the future.

A ANNEX:
BGP SECURITY MEASURES CHECKLIST

BGP SECURITY MEASURES CHECKLIST		
General Information	**Organization name**	*Hint: company name*
	Contact point	*Hint: contact name, email for further questions on this*
	AS	*Hint: Yes, please specify the AS number, or N/A if no AS.* *In the latter case please skip the rest of this form*
BGP Security measure	**Implementation status**	**Explanation**
1. BGP Monitoring & Routing Anomaly Detection	*Hint: Yes, No, Partially*	*Hint: pls explain – and in case you do not implement, or only partially, explain why, which parts not, plans to implement, etc.*
2. BGP Coordination	*Hint: Yes, No, Partially*	*Hint: pls explain – and in case you do not implement, or only partially, explain why, which parts not, plans to implement, etc.*
3. Prefix Filtering	*Hint: Yes, No, Partially*	*Hint: pls explain – and in case you do not implement, or only partially, explain why, which parts not, plans to implement, etc.*
4. BGP AS Path Filtering	*Hint: Yes, No, Partially*	*Hint: pls explain – and in case you do not implement, or only partially, explain why, which parts not, plans to implement, etc.*
5. Bogon Filtering	*Hint: Yes, No, Partially*	*Hint: pls explain – and in case you do not implement, or only partially, explain why, which parts not, plans to implement, etc.*
6. TTL Security (GTSM)	*Hint: Yes, No, Partially*	*Hint: pls explain – and in case you do not implement, or only partially, explain why, which parts not, plans to implement, etc.*
7. RPKI	*Hint: Yes, No, Partially*	*Hint: pls explain – and in case you do not implement, or only partially, explain why, which parts not, plans to implement, etc.*

TP-02-19-361-EN-N

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Network and Information Security
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion Office
Nikolaou Plastira 95
Vassilika Vouton, 700 13, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-294-3
doi: 10.2824/66344