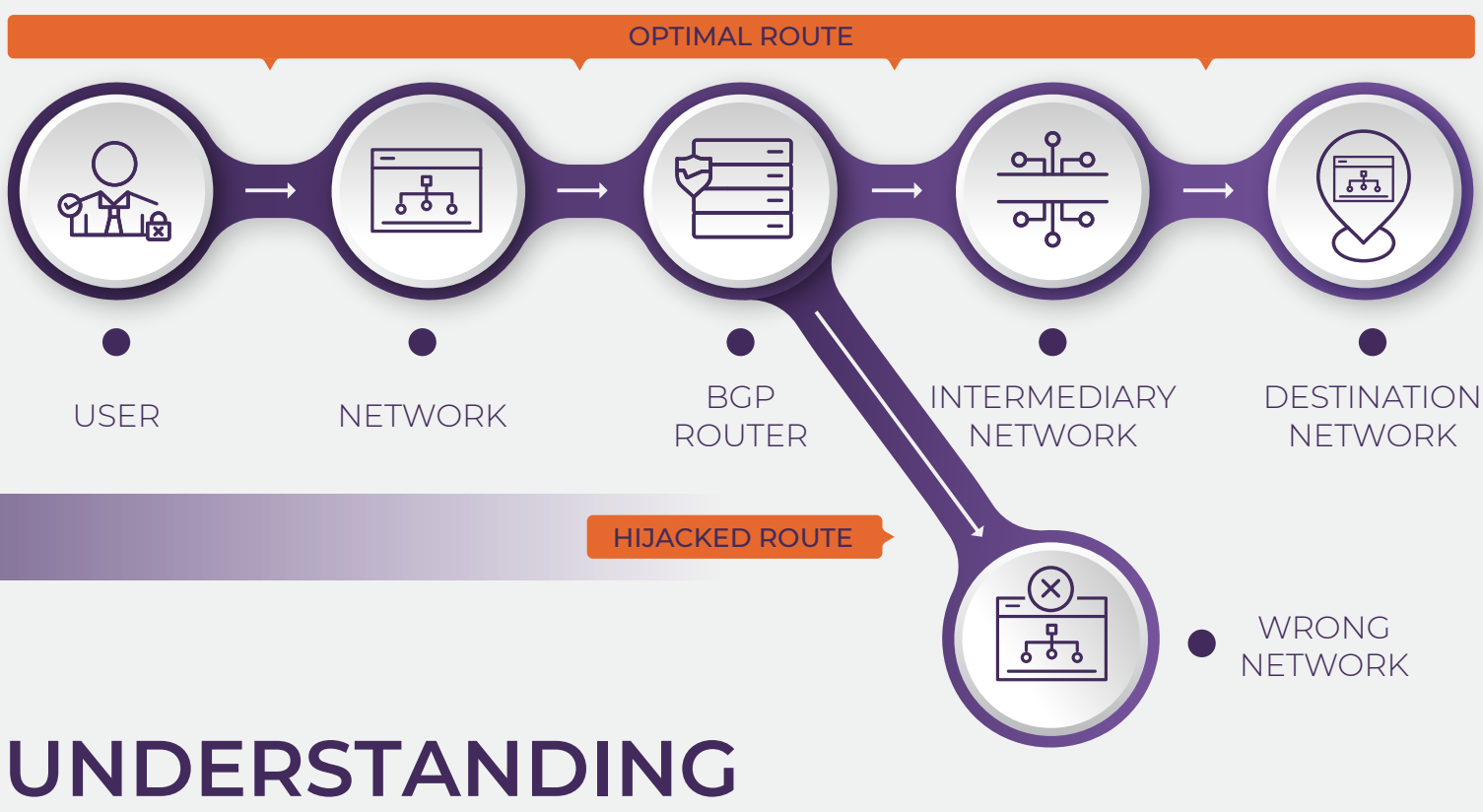
FARSIGHT SECURITY

IP HIJACKING:

When Internet Traffic Takes a Wrong Turn

What is IP Hijacking?

IP hijacking or BGP hijacking is when attackers deliberately and maliciously modify public routing tables. Attackers accomplish this by announcing ownership of IP prefixes that have not actually been assigned to them. If the fraudulent announcement offers a seemingly more optimal route than the legitimate one, traffic may be directed to the attacker.



UNDERSTANDING THE IMPACT

1. BGP (Border Gateway Protocol) is the Internet's routing protocol, used to route traffic efficiently from one IP address to another. BGP assumes that all autonomous systems truthfully relay which IP addresses they own.
2. When traffic is directed to a false path, the most obvious impact is users experience a slower connection to the network.
3. In worse cases, attackers can cause outages to entire networks, disabling an organization's services like a DDos attack would.

THE MECHANICS

INTRA-ORGANIZATION HIJACK

This type is often a non-malicious systemic failure of one sort or another that is restricted to an entity that can choose when and how it handles the failure. Nobody on the public Internet should be affected. This type of failure is more common in large organizations with many different logistical domains.

PUBLIC BGP TABLE HIJACK

Here we span two variations: one where the IP space is hijacked, and another where the ASN and the IP space is hijacked. The former is more common and both can be either accidental as well as malicious. The latter is insidious, mostly because it can look like normal anycast to the rest of the Internet.

CENSORSHIP HIJACK

Less common is the use of a network hijack for censorship, either at the behest of an individual, group, or sovereign nation. This type of hijack differs from the above because its main aim is to disable, restrict, or deny access to specific sources or destinations on the internet.

IN-PATH ASN HIJACK

It is also possible for an attacker to insert a target ASN in announcements they make to the global routing table thereby causing some portion of traffic destined to the target to instead be routed through the attacker's network. This presents a man-in-middle attack.

PUBLIC BGP TABLE HIJACK (VIA ROUTING REGISTRY)

This is the complete hijack scenario. For example, a network administrator went through the trouble to integrate their IRR objects correctly with a registry, but for some reason they find they are no longer in control of the maintainer object. Current recourse for recovery in this scenario is contacting the routing registry and regaining control of the maintainer object.

FOLLOW-UP ATTACKS

In some cases, IP hijacking is only the beginning. The attacker's final objective may be to steal user credentials or exploit their systems. In such cases, the attacker will use the IP hijack to divert your users to malicious sources.

It's critical to be aware of these possibilities and to gather material that could help your organization analyze these attacks such as valuable passive DNS data, Secure Sockets Layer (SSL) certificate history, and full packet captures.

MITIGATE THE RISKS

Farsight's DNS Changes channel provides real-time visibility into changes made to DNS, such as any new record added as well as any new RR change observed. DNS Changes is provided on the Farsight SIE platform. It reports on global changes when existing domains purposely, inadvertently or maliciously:

- Move to a new IP address
- Use different name servers
- Use a new mail exchange
- Start using IPv6 or DNSSEC

Organizations can easily monitor their DNS worldwide and alert on unauthorized changes.

Ready to learn more?

FARSIGHT SECURITY

The best defense is better defense.
Contact Farsight Security today and learn how we can help.

farsightsecurity.com +1-650-489-7919