Dresden University of Technology

HAW HAMBURG

Maynard Koch, Florian Dolzmann, Thomas C. Schmidt, Matthias Wählisch

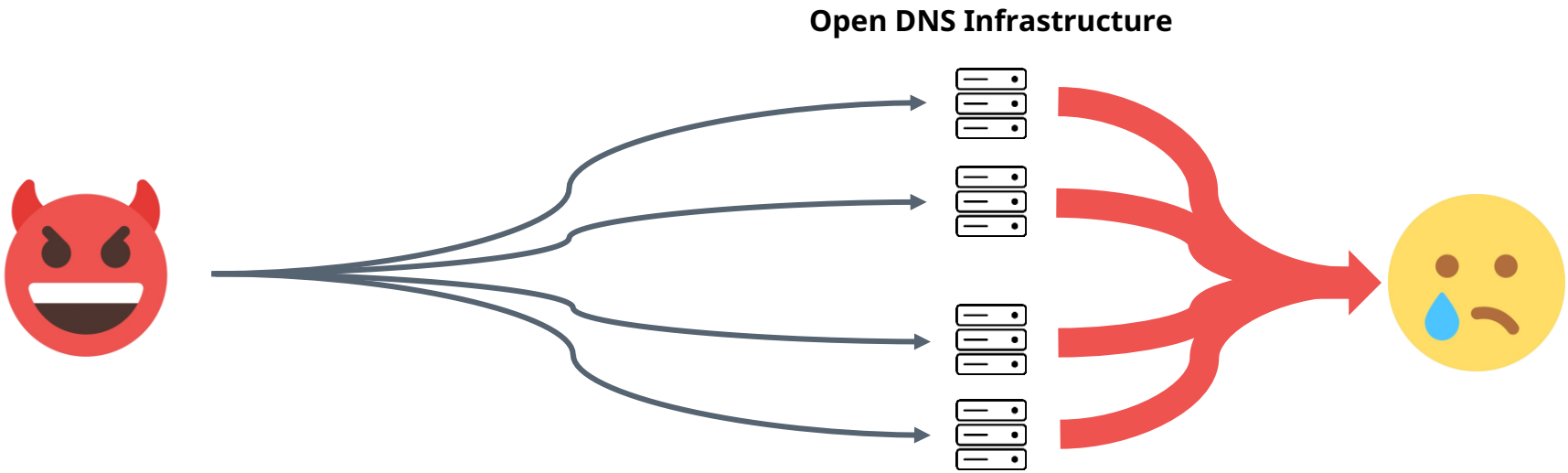
Forward to Hell?
On the Potentials of Misusing Transparent DNS Forwarders in Reflective Amplification Attacks

ACM CCS 2025, Taipei, Taiwan // October 13-17, 2025

DNS Distributed Denial-of-Service (DDoS) Attacks are a Common Threat

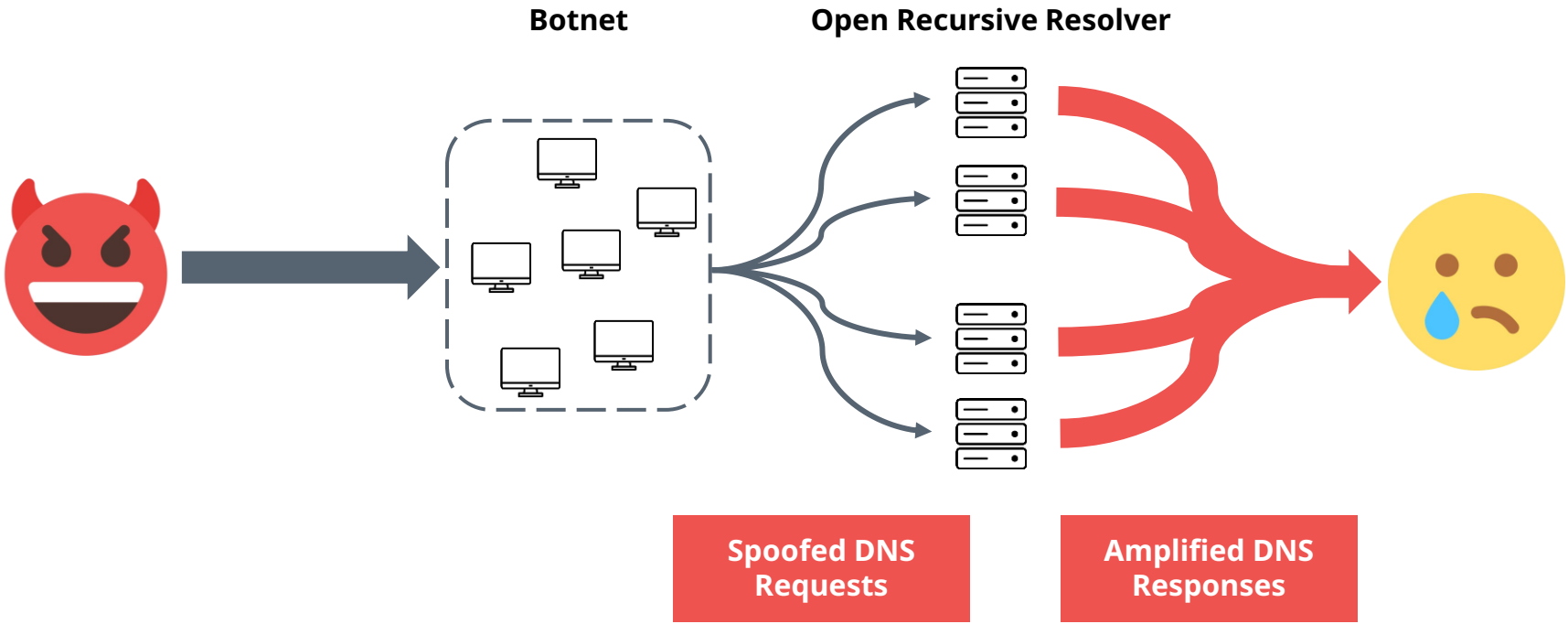
The Open DNS (ODNS) Infrastructure is Misused in DDoS Attacks

Open components serve as reflectors or amplifiers.



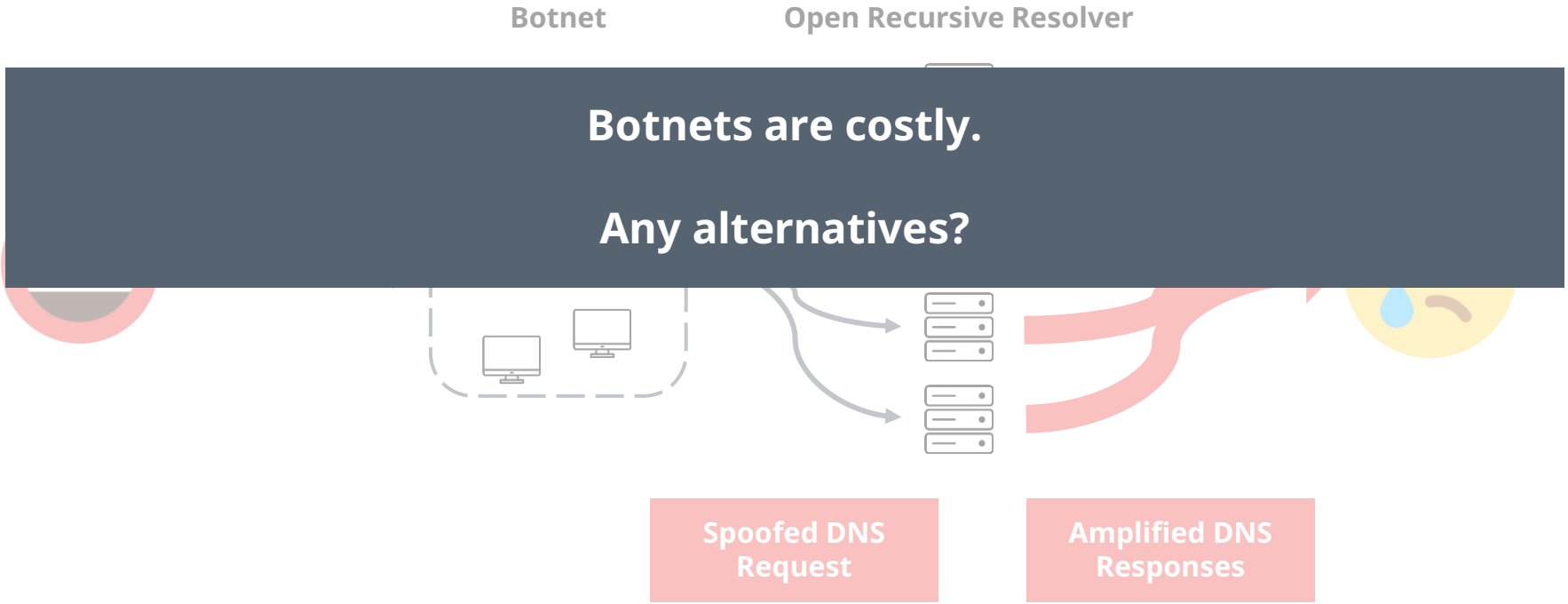
Potential Misuse Scenario of Open Recursive Resolvers

To run a distributed attack, the attacker needs access to a botnet.



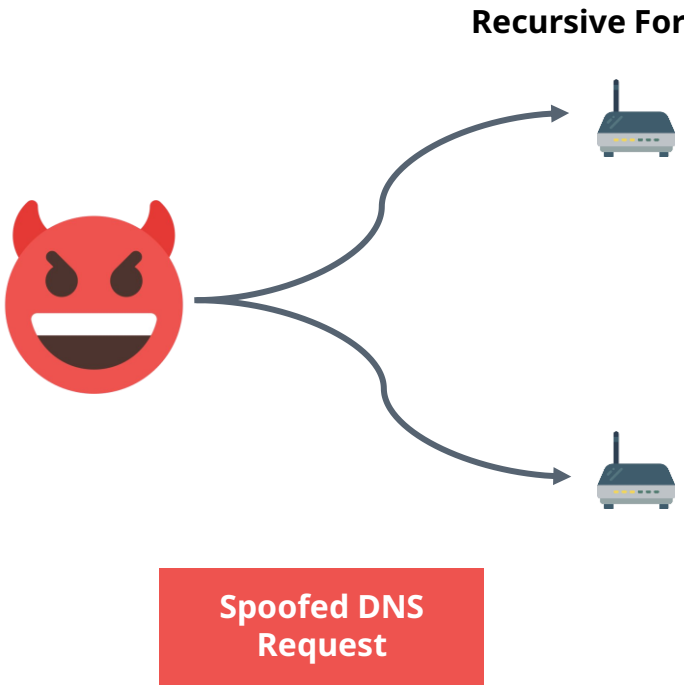
Potential Misuse Scenario of Open Recursive Resolvers

To run a distributed attack, the attacker needs access to a botnet.



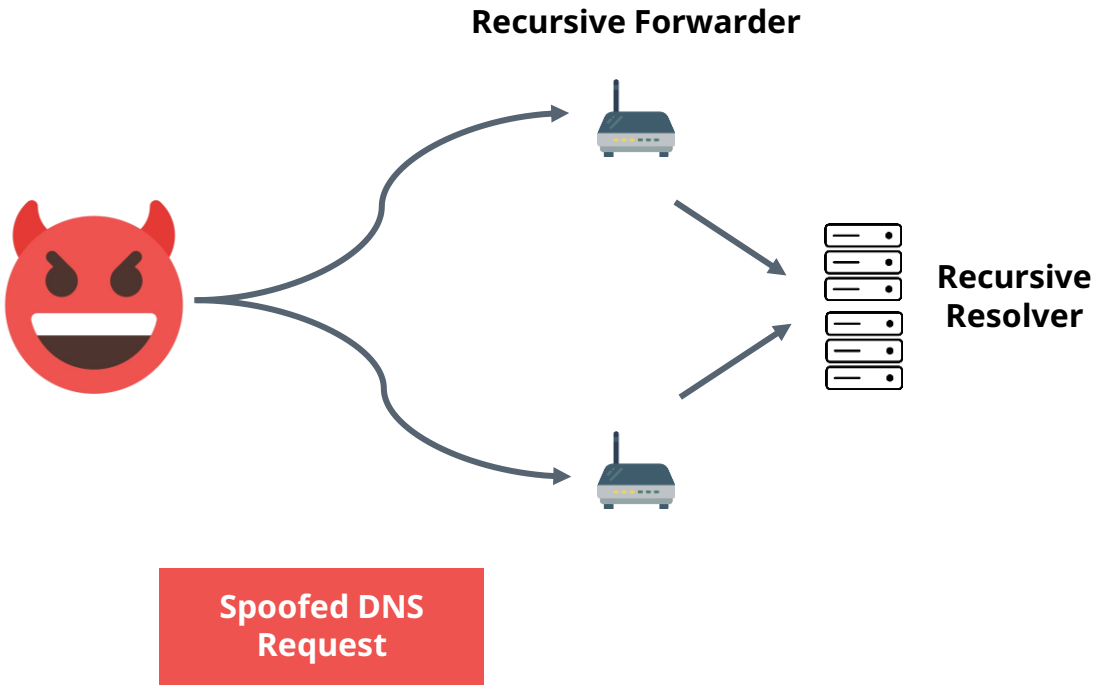
Potential Misuse Scenario of Open Recursive Forwarders

Forwarders are globally distributed, enabling distributed attacks w/o a botnet.



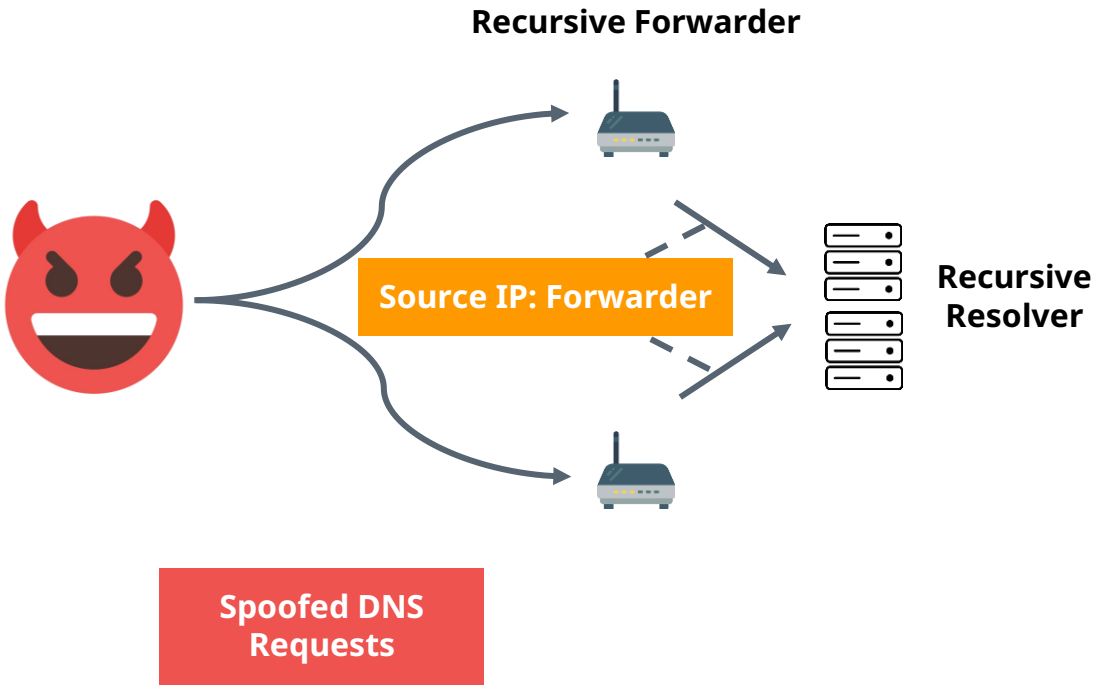
Potential Misuse Scenario of Open Recursive Forwarders

Forwarders are globally distributed, enabling distributed attacks w/o a botnet.



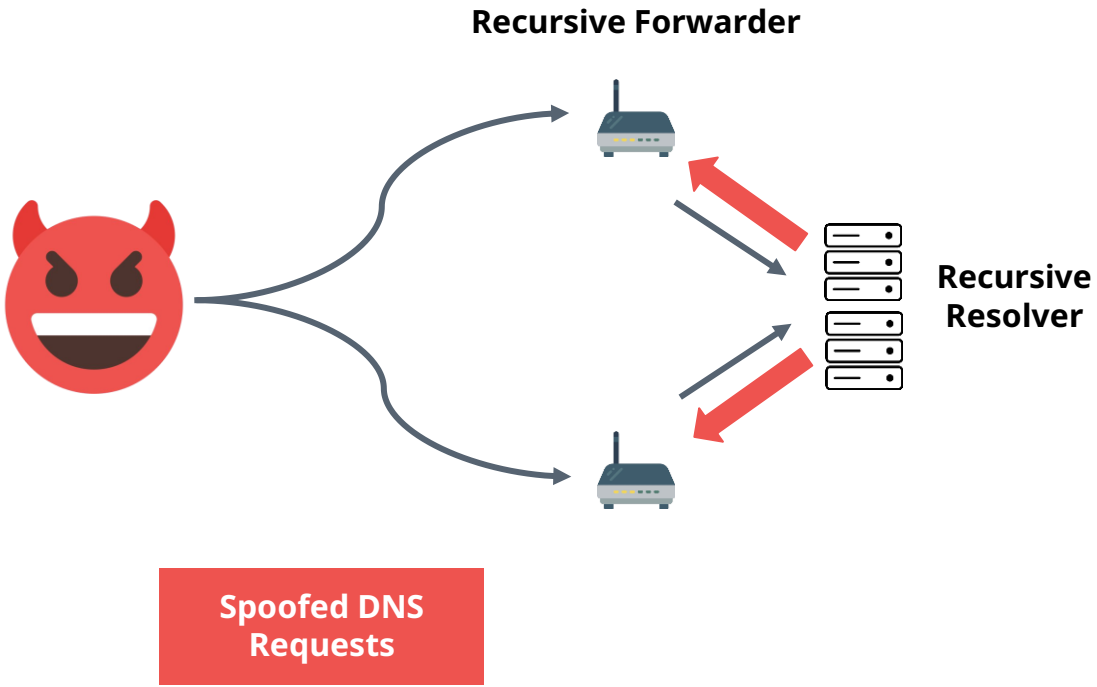
Potential Misuse Scenario of Open Recursive Forwarders

Forwarders are globally distributed, enabling distributed attacks w/o a botnet.



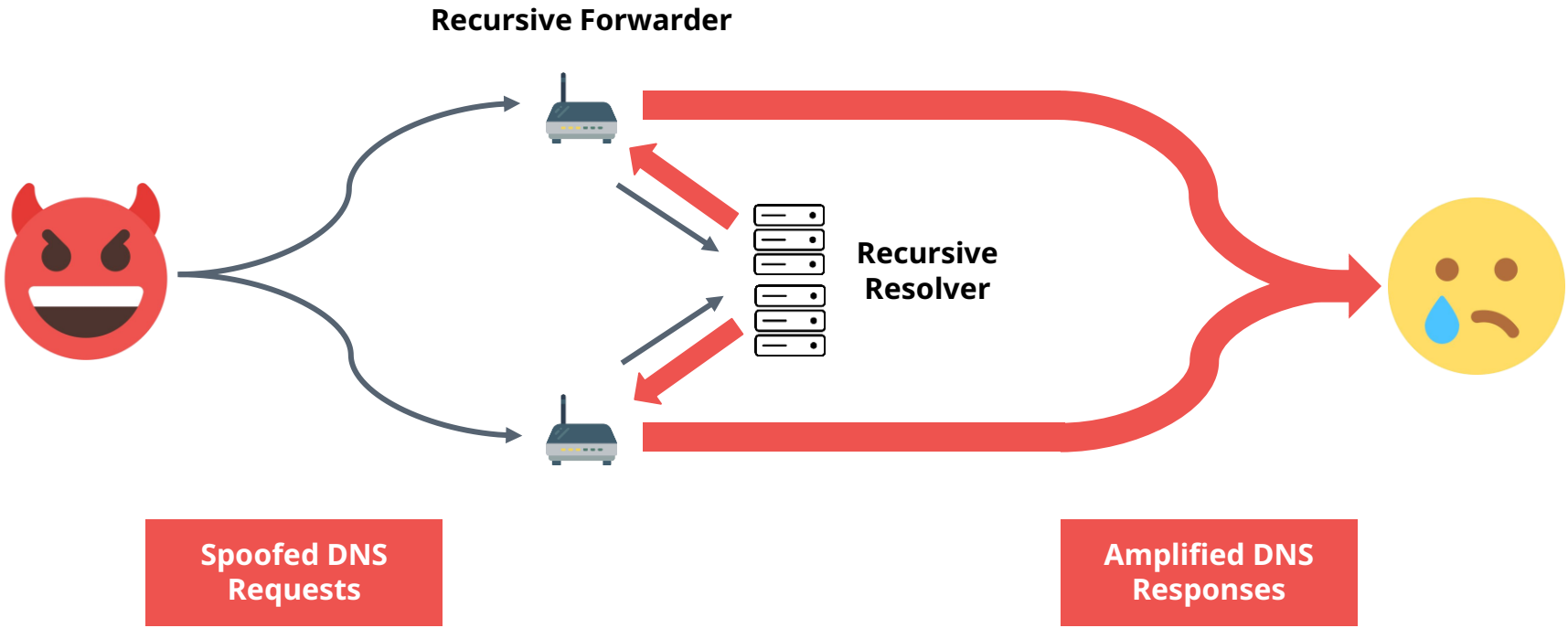
Potential Misuse Scenario of Open Recursive Forwarders

Forwarders are globally distributed, enabling distributed attacks w/o a botnet.



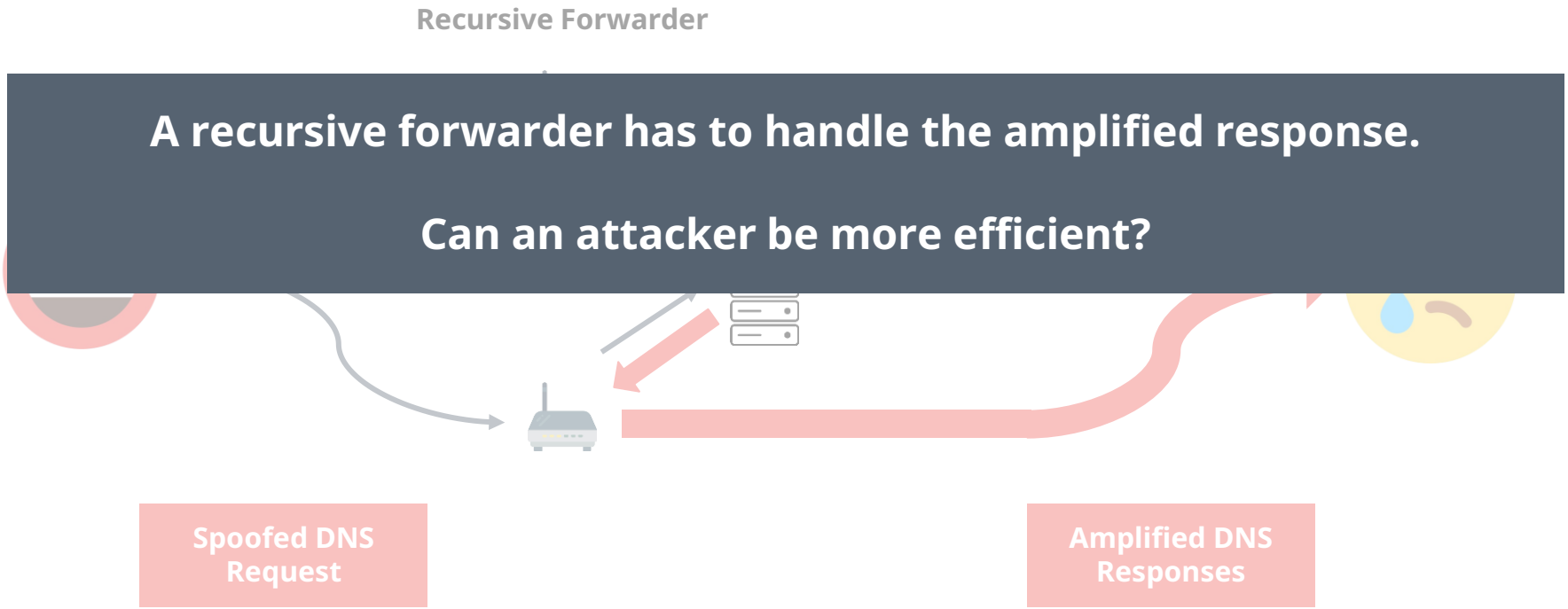
Potential Misuse Scenario of Open Recursive Forwarders

Forwarders are globally distributed, enabling distributed attacks w/o a botnet.



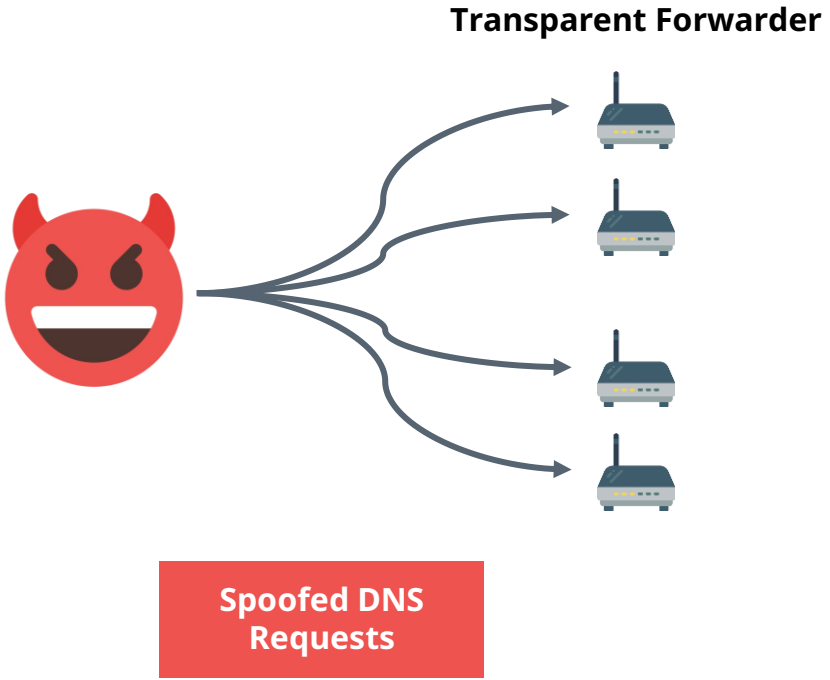
Potential Misuse Scenario of Open Recursive Forwarders

Forwarders are globally distributed, enabling distributed attacks w/o a botnet.



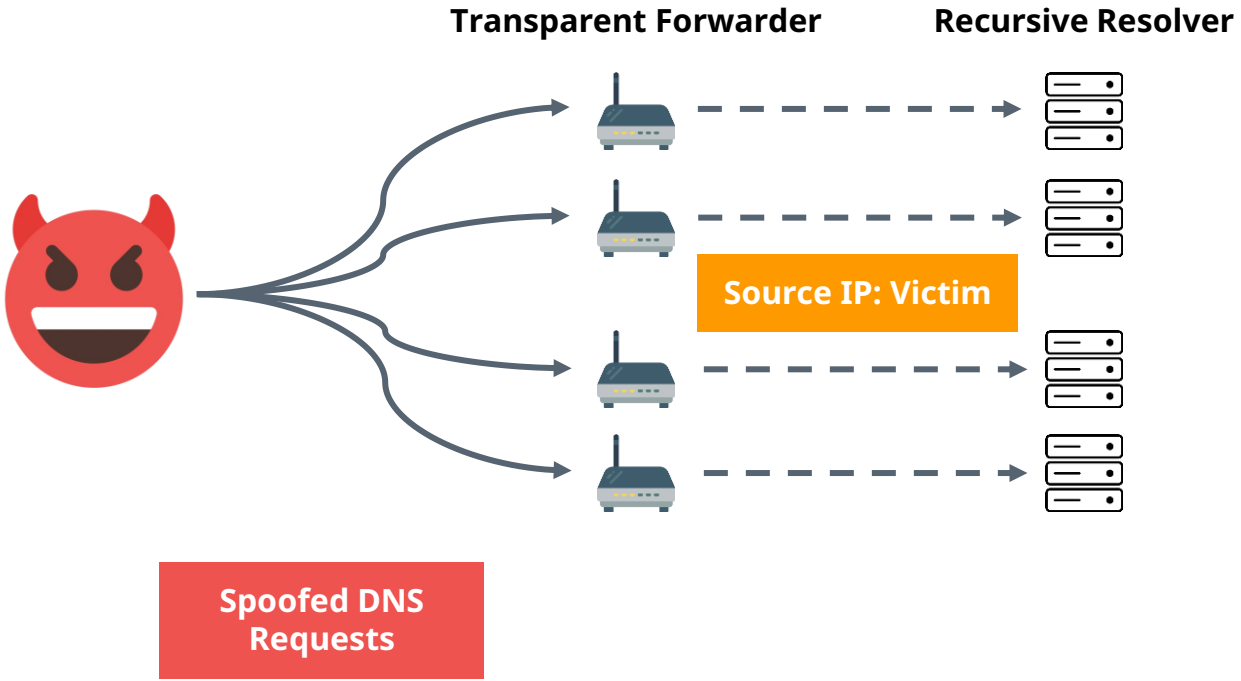
Transparent DNS Forwarders

Misconfigured devices, not intentionally deployed.



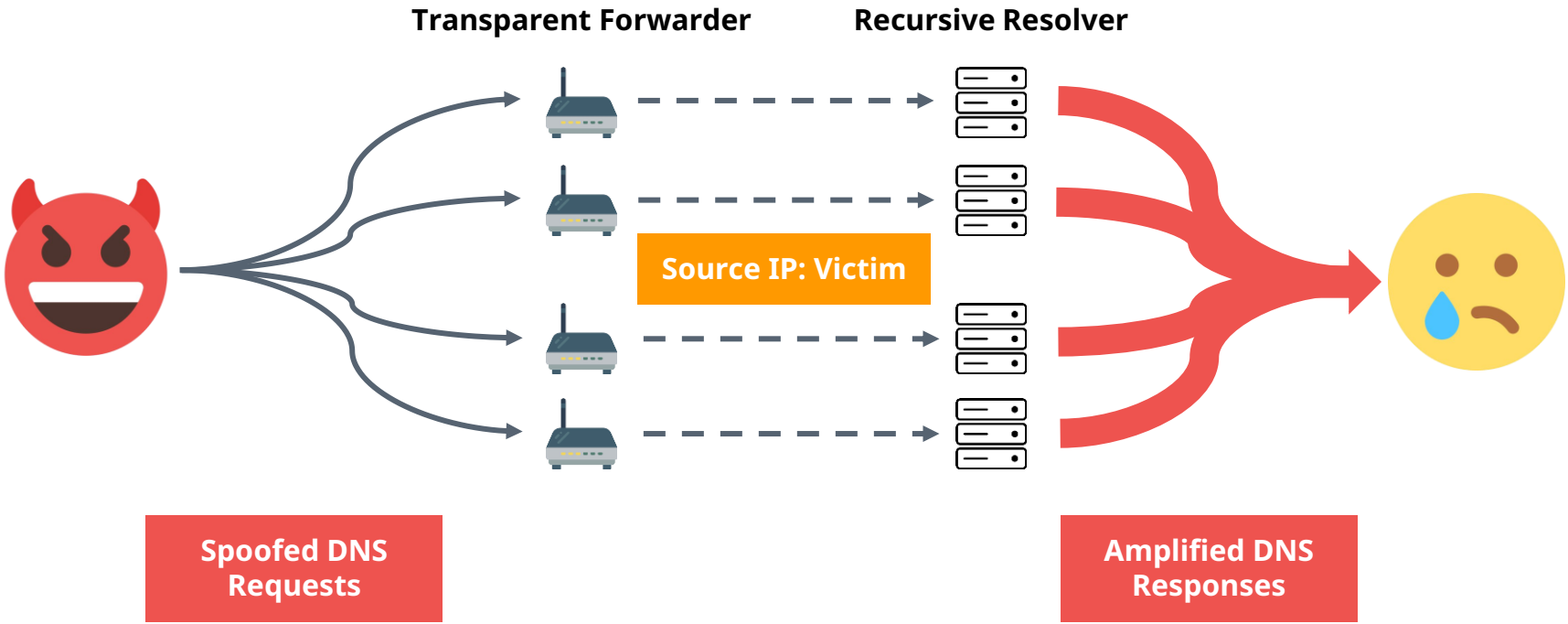
Transparent DNS Forwarders

They do not rewrite the source IP address of the arriving packet.



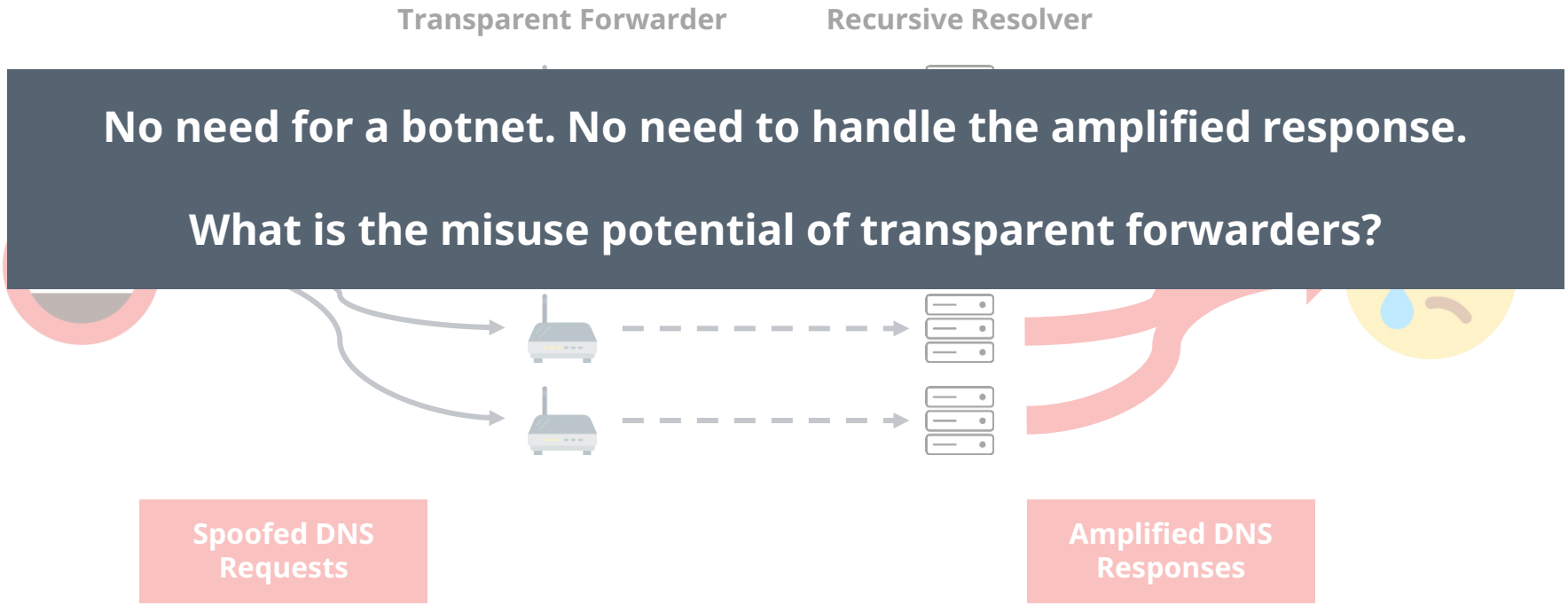
Transparent DNS Forwarders

The recursive resolver allegedly receives a DNS request from the DDoS target.



Transparent DNS Forwarders

The recursive resolver allegedly receives a DNS request from the DDoS target.

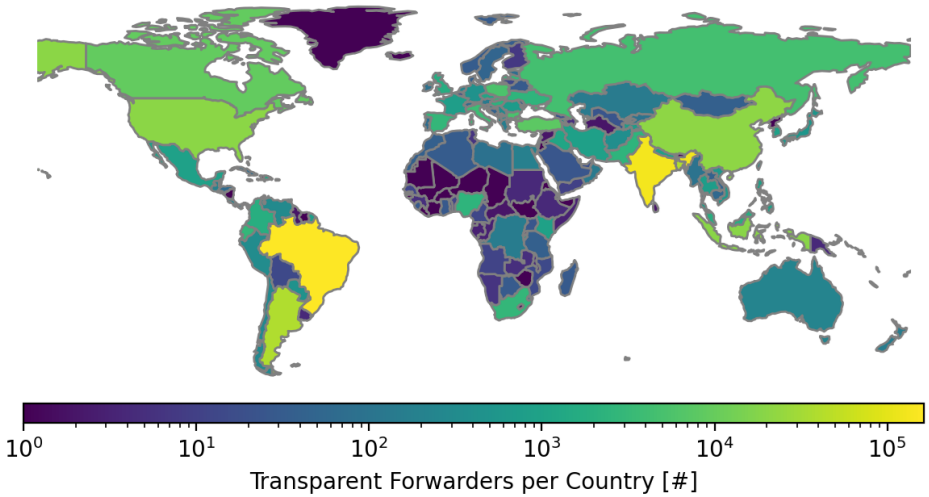


What is this talk about?

1. **Additional Attack Infrastructure**
2. Higher Efficiency in Potential Attacks
3. Avoiding Local Rate Limits by Orchestrating Transparent Forwarders
4. Responsible Disclosure and Mitigation Options

Additional Attack Infrastructure – Geographical Distribution

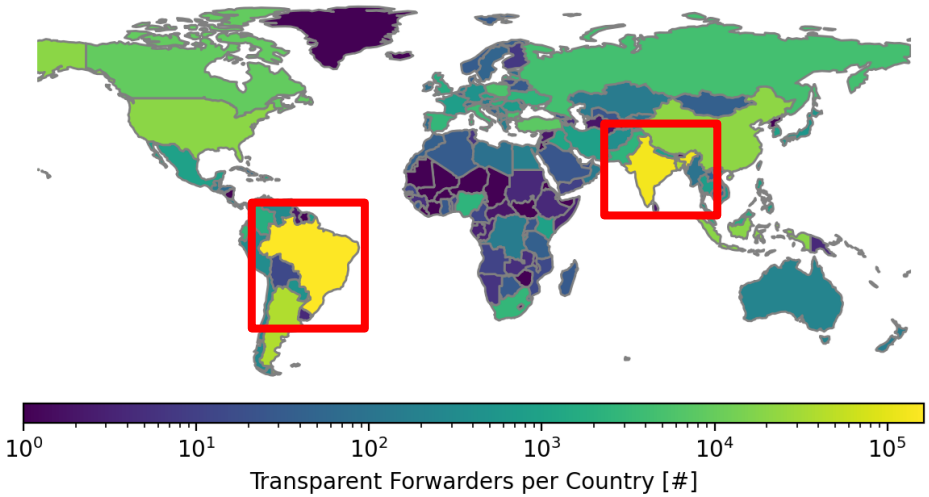
More than 30% of the open DNS infrastructure are transparent forwarders.



Large number of devices. 540k of all open DNS components are **transparent forwarders**.

Additional Attack Infrastructure – Geographical Distribution

Brazil and India host >50% of all transparent forwarders.

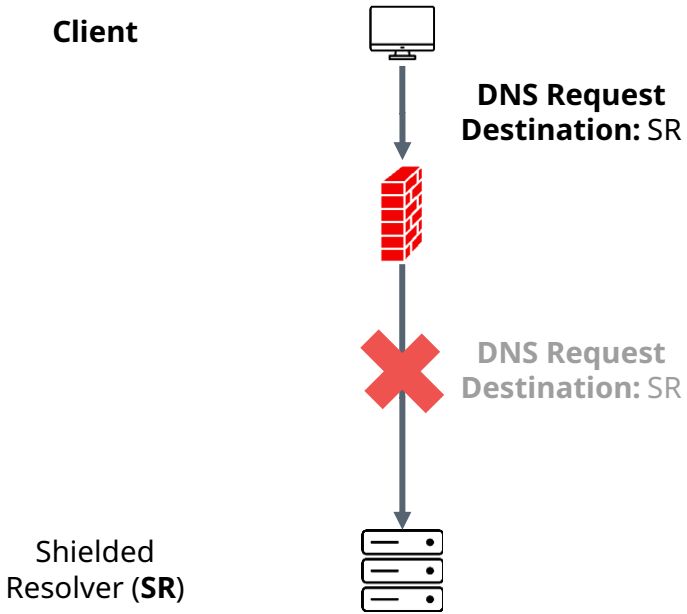


Large number of devices. 540k of all open DNS components are **transparent forwarders**.

Widely distributed with regional bias. Transparent forwarders can be found in **175 countries**, most of them are active in Brazil and India.

Additional Attack Infrastructure – Shielded Resolvers

Transparent forwarders enable access to shielded resolvers.

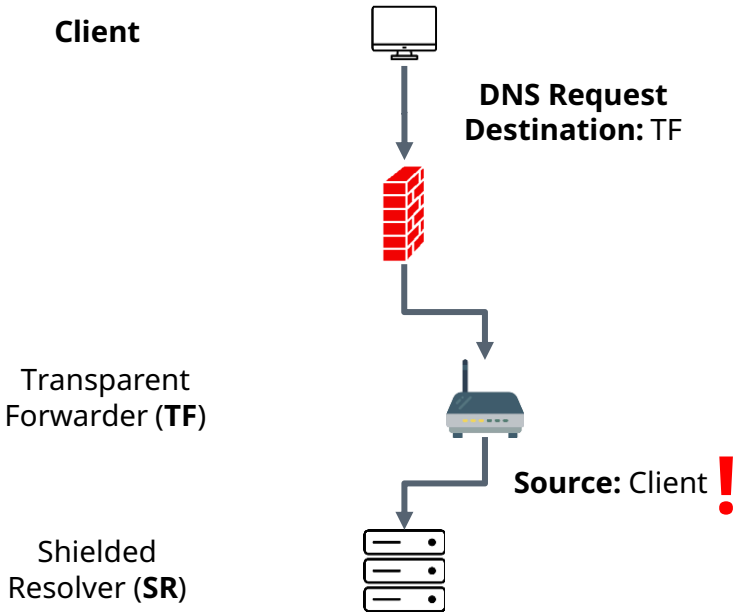


Shielded resolvers should only be accessible from the internal network.

Firewall at the network border filters requests that directly target the shielded resolver.

Additional Attack Infrastructure – Shielded Resolvers

Transparent forwarders enable access to shielded resolvers.



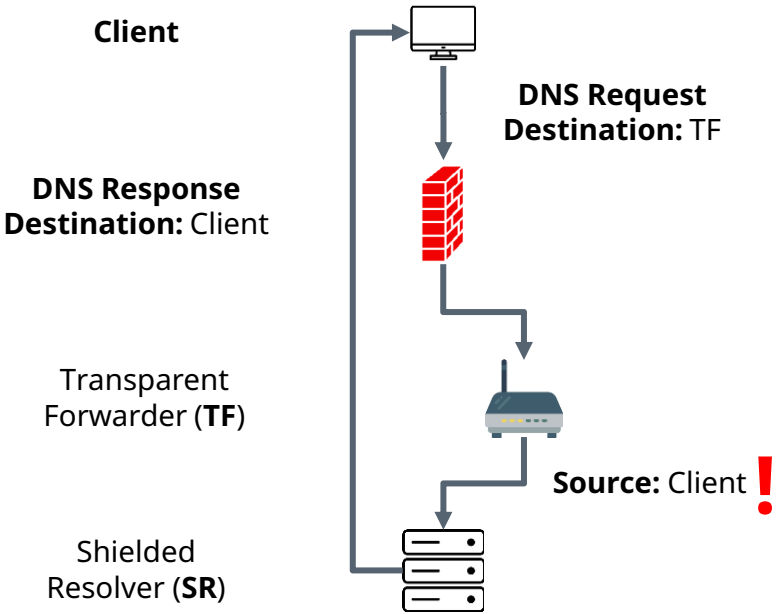
Shielded resolvers should only be accessible from the internal network.

Firewall at the network border filters requests that directly target the shielded resolver.

The transparent forwarder is not affected by the firewall rules at the network border.

Additional Attack Infrastructure – Shielded Resolvers

Transparent forwarders enable access to shielded resolvers.



Shielded resolvers should only be accessible from the internal network.

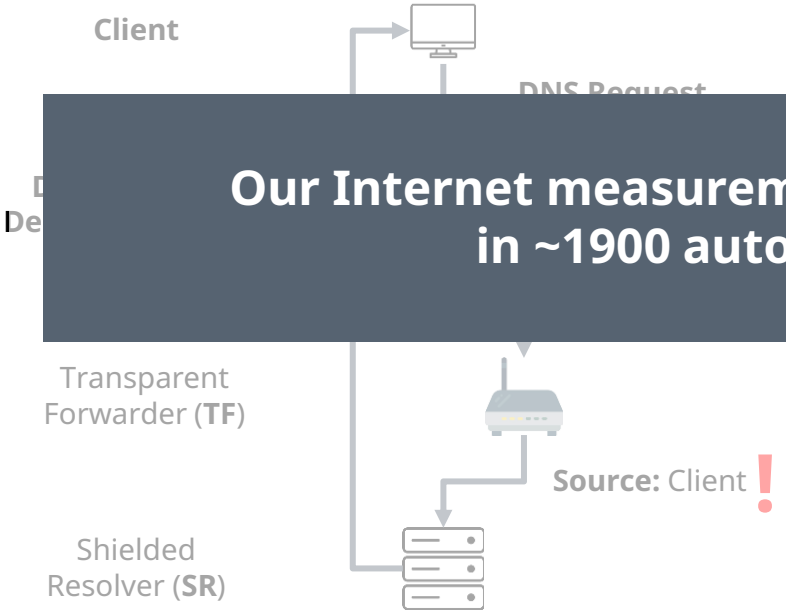
Firewall at the network border filters requests that directly target the shielded resolver.

The transparent forwarder is not affected by the firewall rules at the network border.

No properly configured firewall at the resolver, hence the client receives a valid DNS response.

Additional Attack Infrastructure – Shielded Resolvers

Transparent forwarders enable access to shielded resolvers.



Our Internet measurements reveal 30k shielded resolvers in ~1900 autonomous systems (ASes).

Shielded resolvers should only be

The transparent forwarder is not affected by the firewall rules at the network border.

No properly configured firewall at the resolver, hence the client receives a valid DNS response.

What is this talk about?

1. Additional Attack Infrastructure
2. **Higher Efficiency in Potential Attacks**
3. Avoiding Local Rate Limits by Orchestrating Transparent Forwarders
4. Responsible Disclosure and Mitigation Options

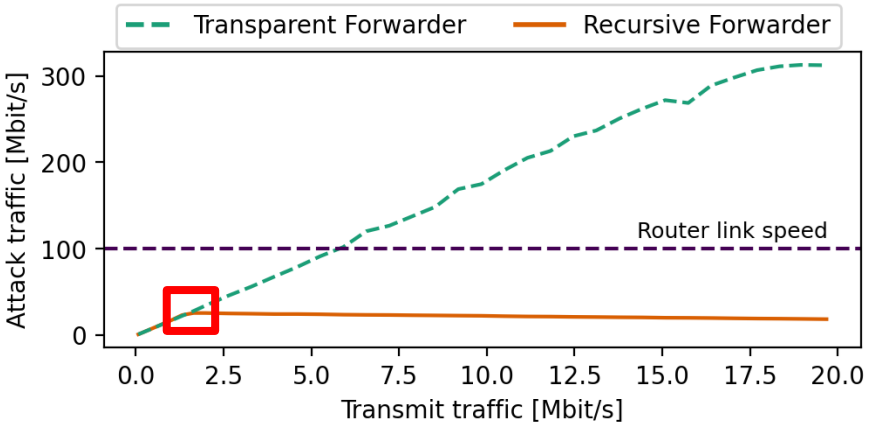
Transparent Forwarders Allow For More Attack Traffic

They do not need to handle the amplified DNS response.

Testbed. We use a MikroTik RB750Gr3 router (i) as a transparent forwarder and (ii) as a recursive forwarder to show the advantage of transparent forwarders.

Transparent Forwarders Allow For More Attack Traffic

Recursive forwarder quickly reaches its maximum attack rate.

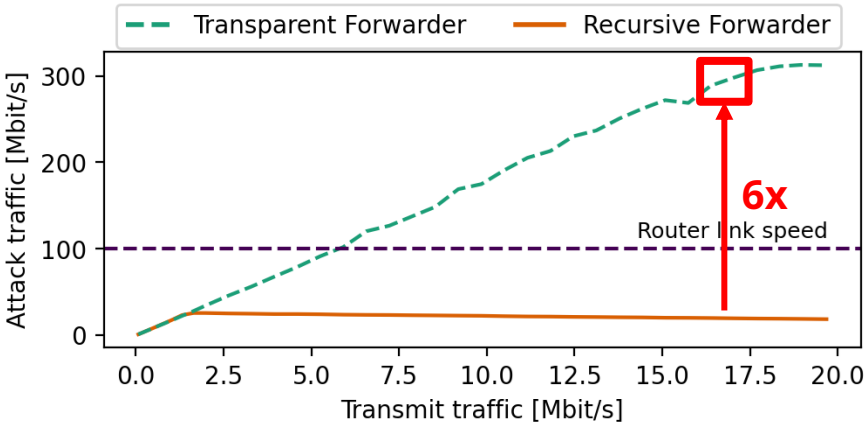


Testbed. We use a MikroTik RB750Gr3 router (i) as a transparent forwarder and (ii) as a recursive forwarder to show the advantage of transparent forwarders.

Recursive forwarder. The router already runs into resource limitations at 1.5Mbit/s of query traffic, resulting in **≈50Mbit/s** of attack traffic.

Transparent Forwarders Allow For More Attack Traffic

Transparent forwarder generates more than 300Mbit/s (6x) attack traffic.



Testbed. We use a MikroTik RB750Gr3 router (i) as a transparent forwarder and (ii) as a recursive forwarder to show the advantage of transparent forwarders.

Recursive forwarder. The router already runs into resource limitations at 1.5Mbit/s of query traffic, resulting in **≈50Mbit/s** of attack traffic.

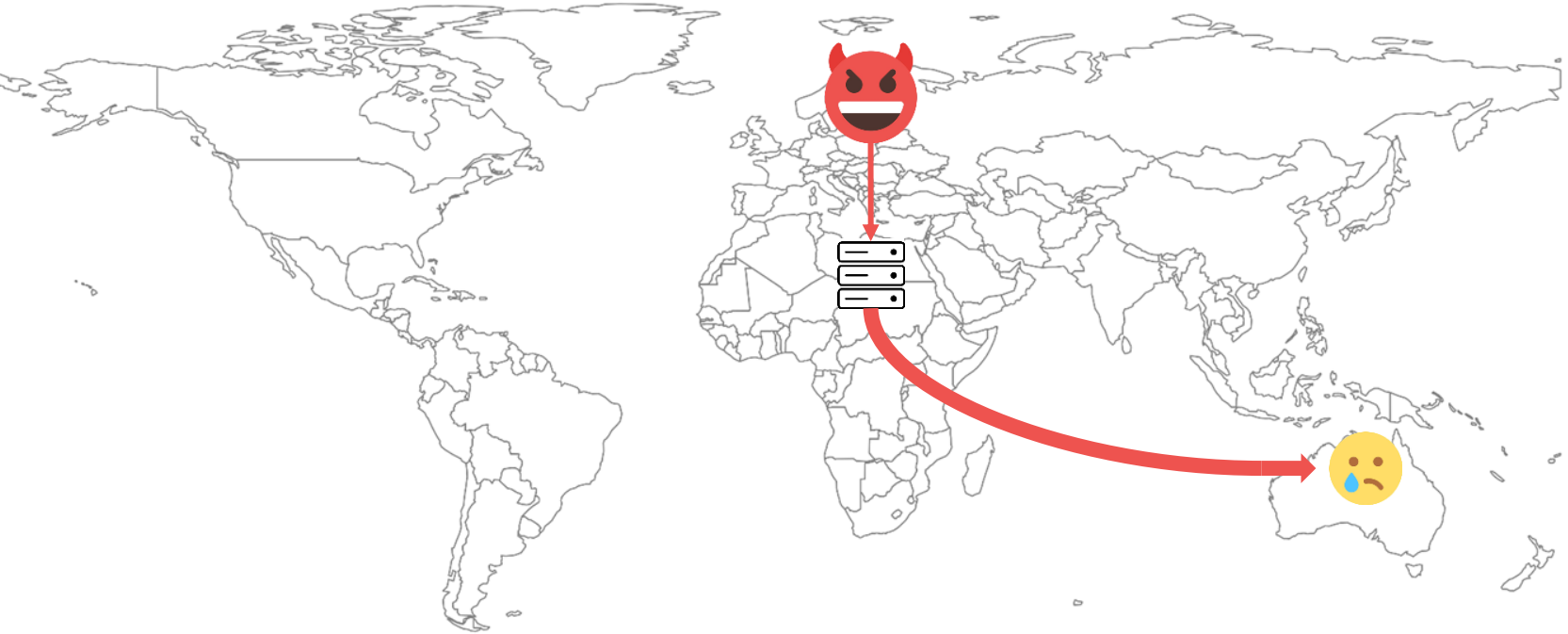
Transparent forwarder. We reach more than **300Mbit/s** of attack traffic before running into resource limitations of the MikroTik router.

What is this talk about?

1. Additional Attack Infrastructure
2. Higher Efficiency in Potential Attacks
3. **Avoiding Local Rate Limits by Orchestrating Transparent Forwarders**
4. Responsible Disclosure and Mitigation Options

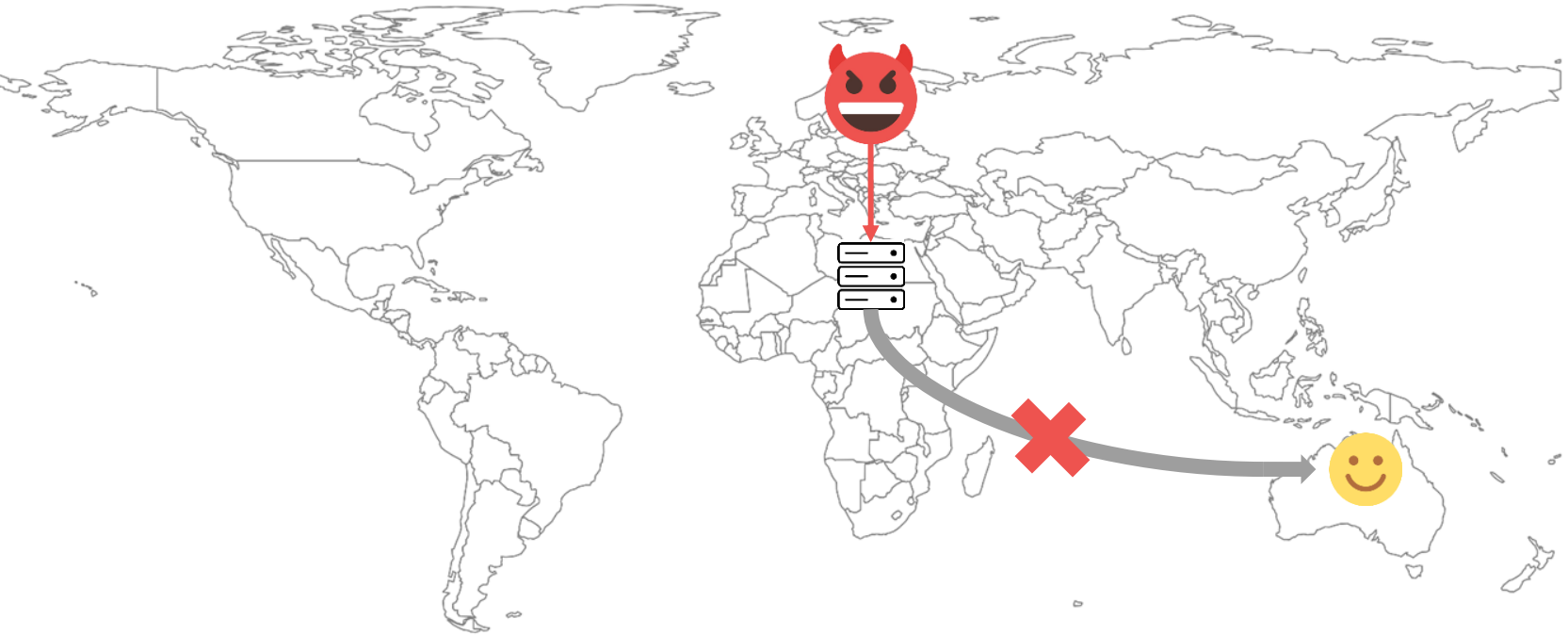
The Attacker Controls a Single Vantage Point

Without a botnet, the attacker reaches only a single point of presence (PoP).



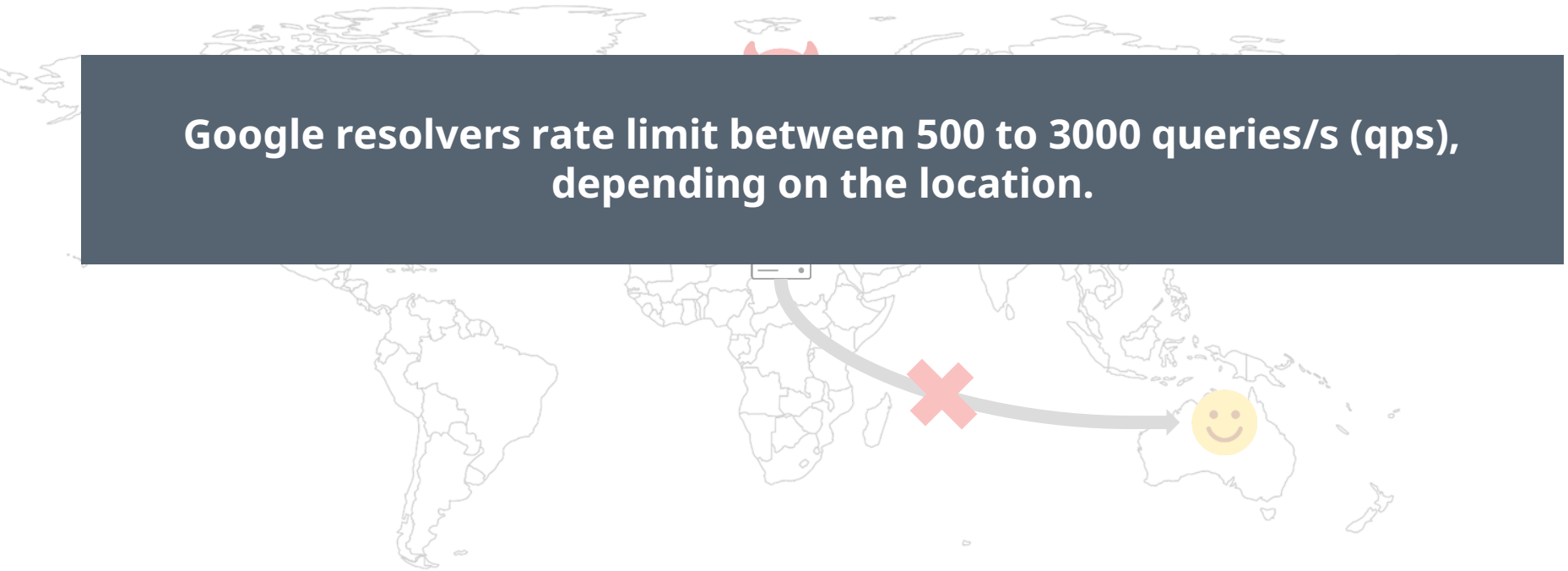
The Attacker Controls a Single Vantage Point

Local rate limits prevent an effective amplification attack.



The Attacker Controls a Single Vantage Point

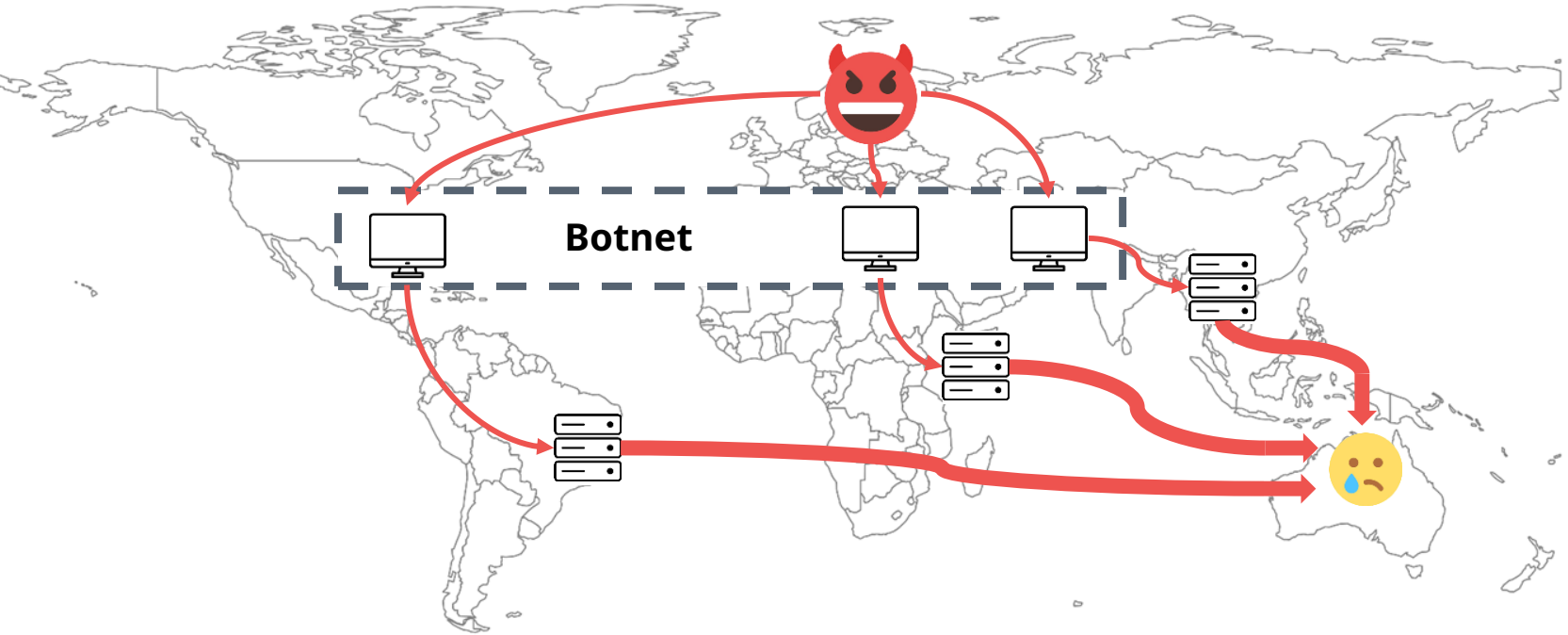
Local rate limits prevent an effective amplification attack.



Google resolvers rate limit between 500 to 3000 queries/s (qps), depending on the location.

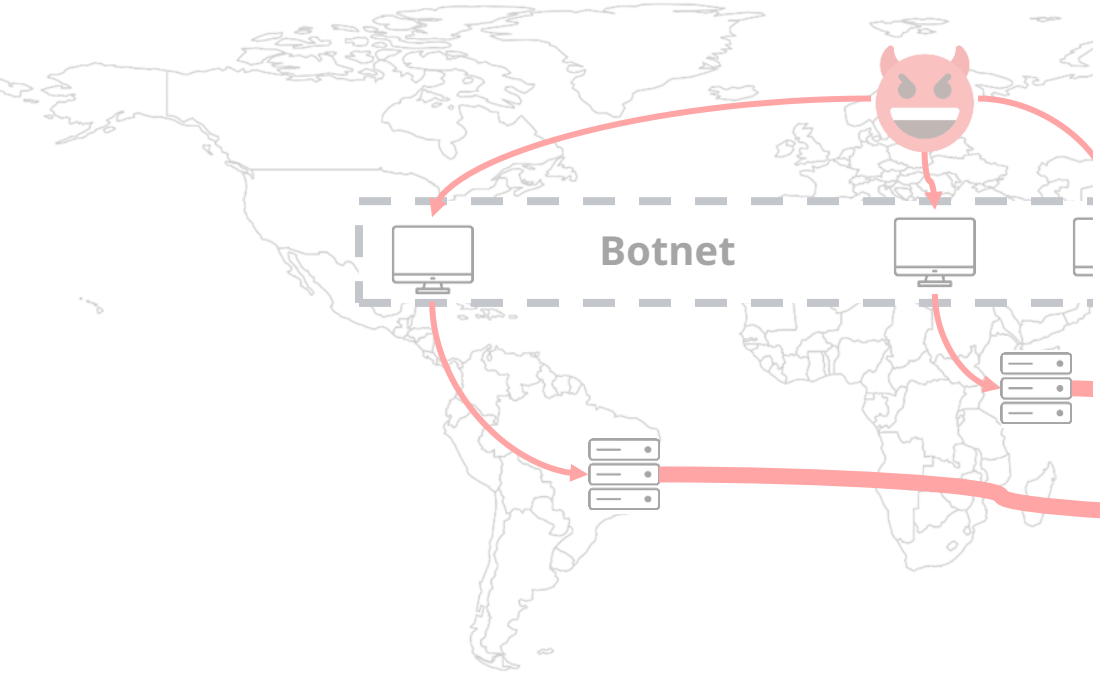
The Attacker Controls a Botnet

Local rate limits can be avoided through global distribution.



Transparent Forwarders Relay Requests to Anycast Deployments

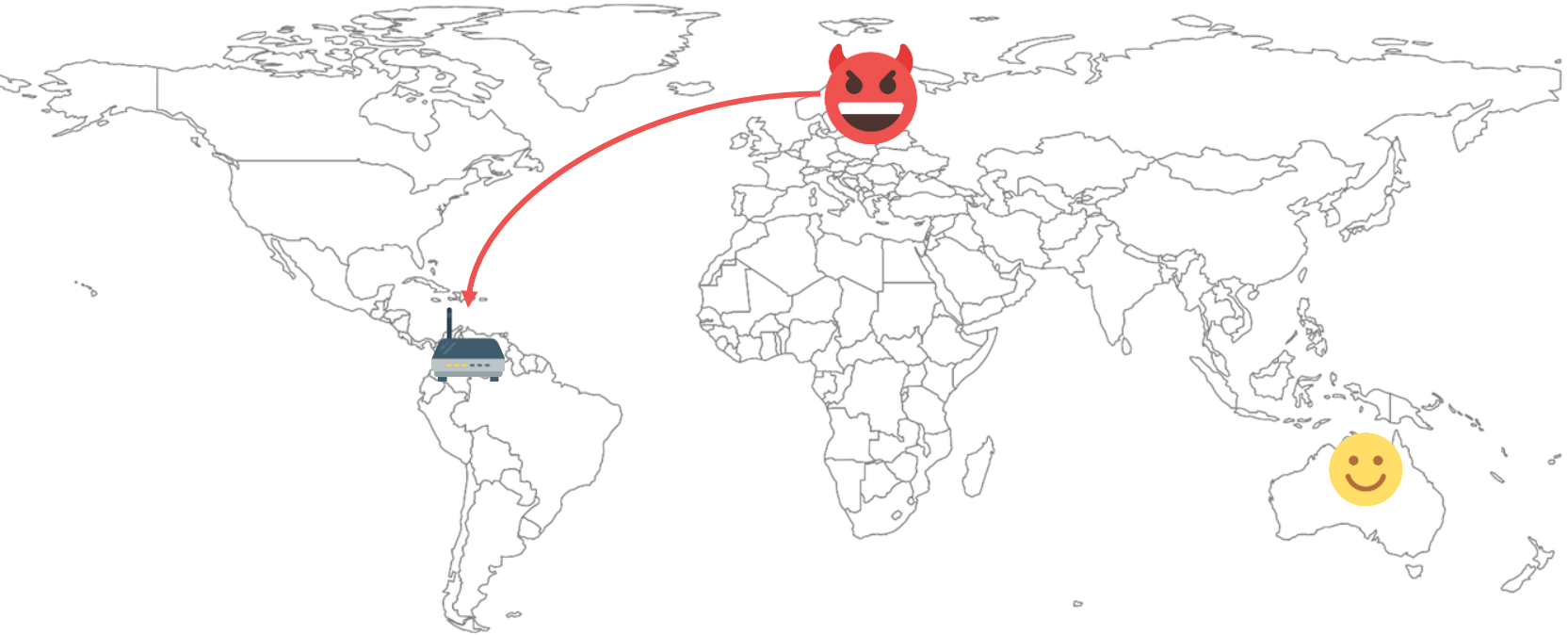
An attacker can exploit the anycast infrastructure.



Public Resolver		Transparent Forwarders Using Public Resolvers	
IP Address	Provider	[#]	[%]
8.8.8.8	Google	341,447	64.25
1.1.1.1	Cloudflare	48,313	9.09
208.67.222.222	OpenDNS	14,464	2.72
8.8.4.4	Google	14,115	2.66
223.29.207.110	Meghbela	11,789	2.22
83.220.169.155	Comss.one DNS	2047	0.39
178.233.140.109	Turksat	1790	0.34
203.147.91.2	Meghbela	1634	0.31
1.0.0.1	Cloudflare	1196	0.23
103.88.88.88	DNS Bersama	1007	0.19

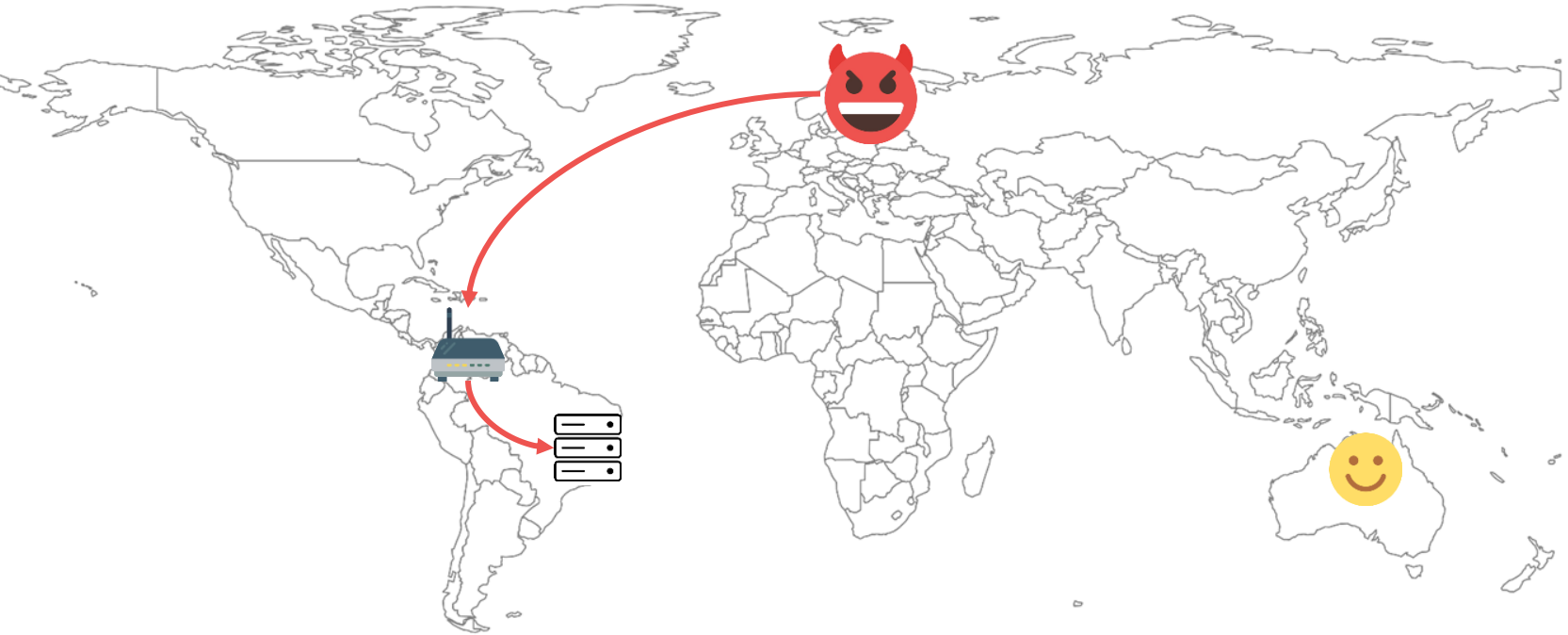
Transparent Forwarders can be Utilized to Circumvent Rate Limiting

An attacker can orchestrate transparent forwarders



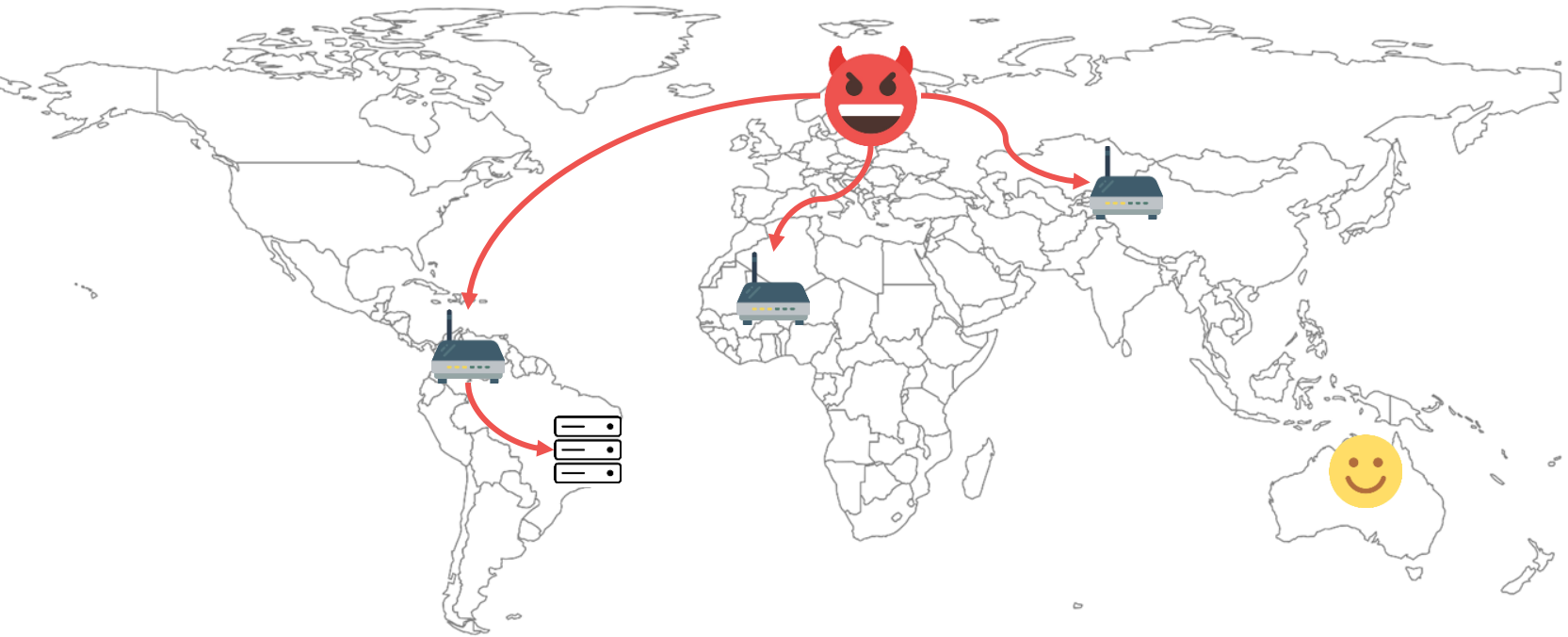
Transparent Forwarders can be Utilized to Circumvent Rate Limiting

An attacker can orchestrate transparent forwarders to reach multiple PoP instances of public DNS providers such as Google.



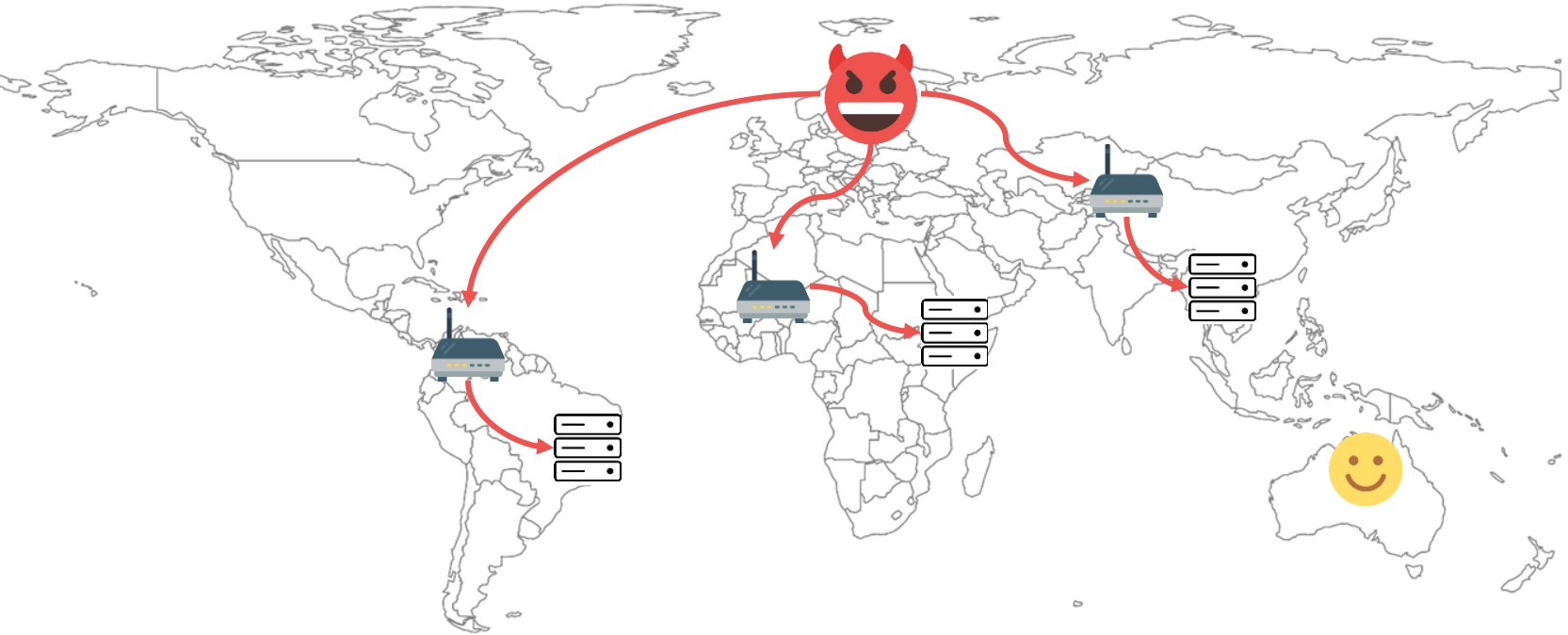
Transparent Forwarders can be Utilized to Circumvent Rate Limiting

A set of transparent forwarders is selected



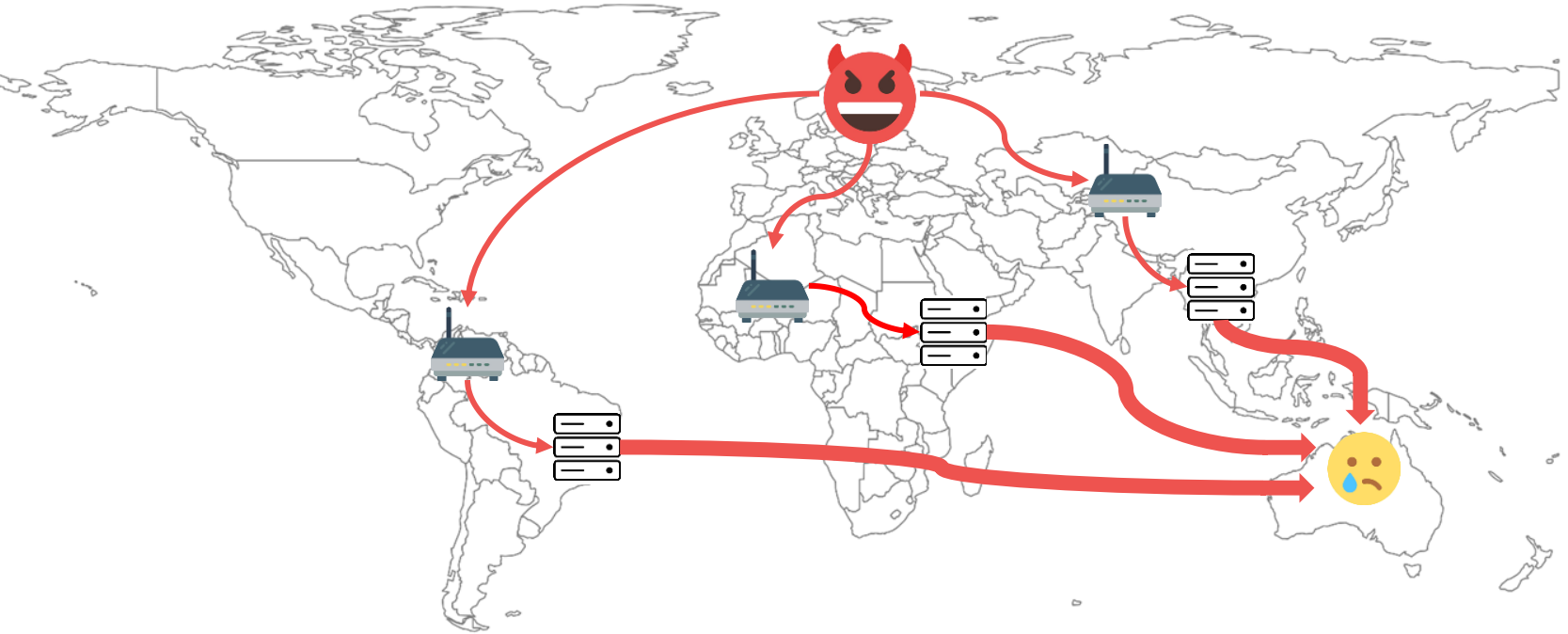
Transparent Forwarders can be Utilized to Circumvent Rate Limiting

A set of transparent forwarders is selected that hits multiple PoPs.



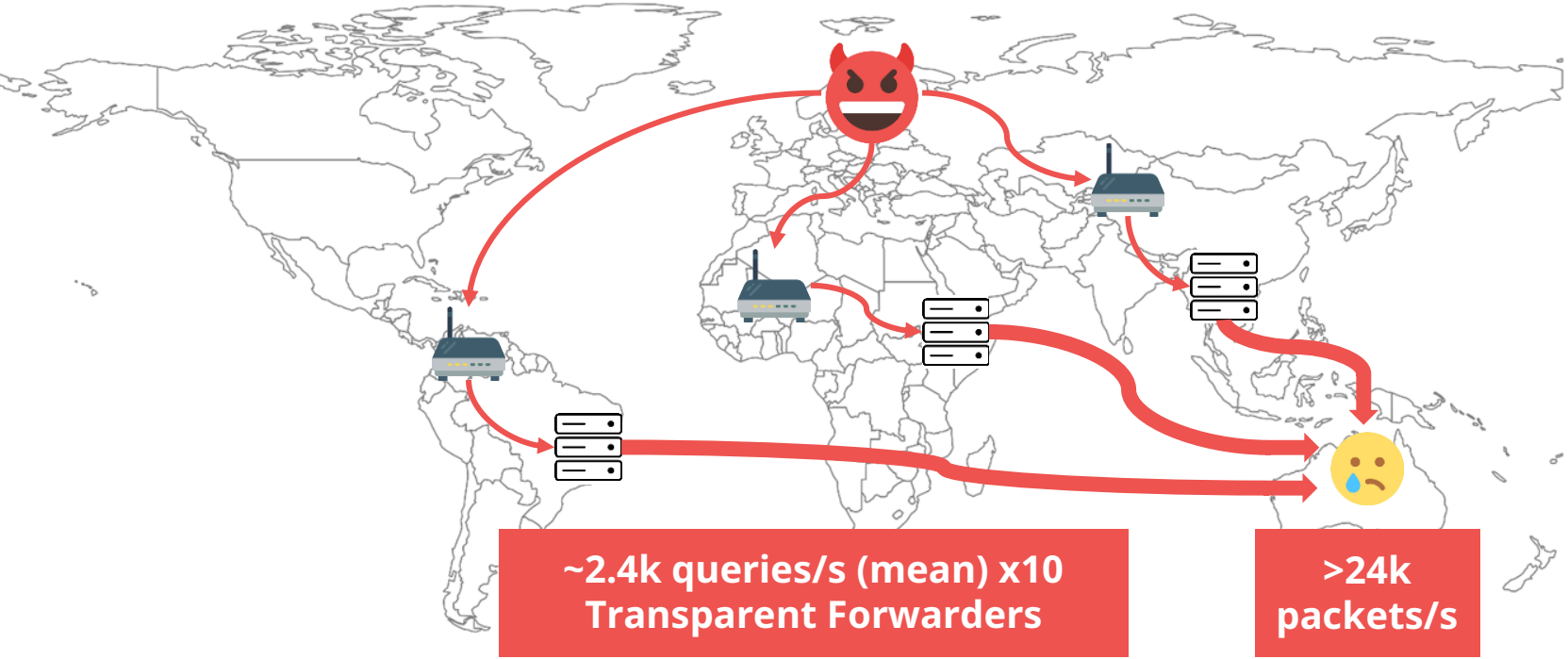
Transparent Forwarders can be Utilized to Circumvent Rate Limiting

The victim receives a flood of DNS responses from, e.g., Google.



Transparent Forwarders can be Utilized to Circumvent Rate Limiting

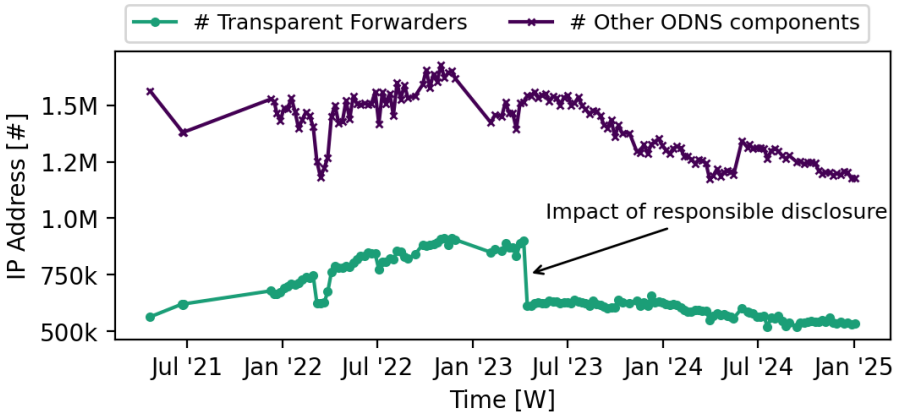
Using Internet-wide measurements, we can show an amplification factor of up to 14 by orchestrating 10 transparent forwarders.



What is this talk about?

1. Additional Attack Infrastructure
2. Higher Efficiency in Potential Attacks
3. Avoiding Local Rate Limits by Orchestrating Transparent Forwarders
4. **Responsible Disclosure and Mitigation Options**

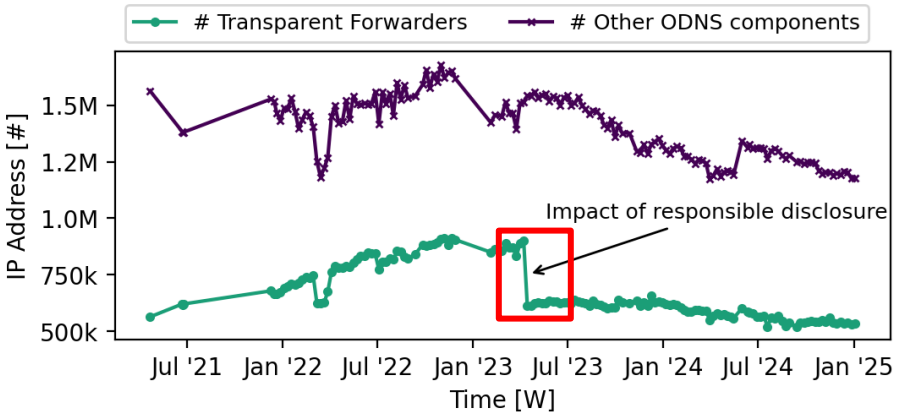
Responsible Disclosure to Reduce the Impact of Transparent Forwarders



Contacting operators. We constantly try to get in touch with operators of networks that host transparent forwarders.

Reducing the impact. Our responsible disclosure removed >250k transparent forwarders from the threat landscape.

Responsible Disclosure to Reduce the Impact of Transparent Forwarders



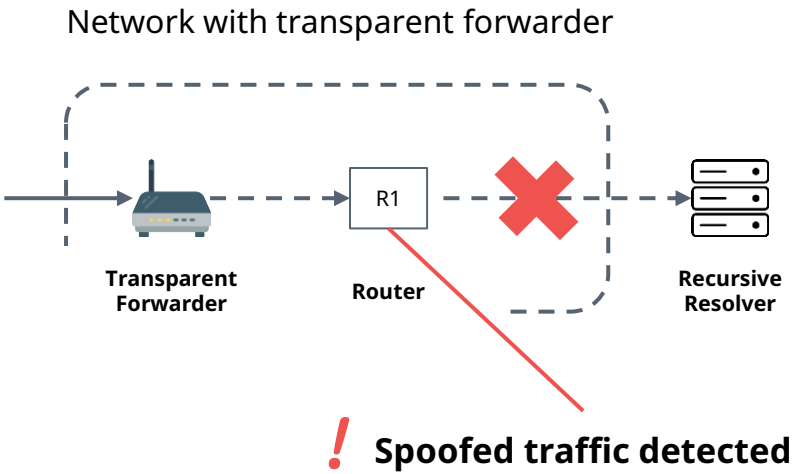
Contacting operators. We constantly try to get in touch with operators of networks that host transparent forwarders.

Reducing the impact. Our responsible disclosure removed >250k transparent forwarders from the threat landscape.

A large European ISP fixed their firewall rules to prevent unrestricted access from transparent forwarders.

Operators should verify and update their firewall rules if necessary!

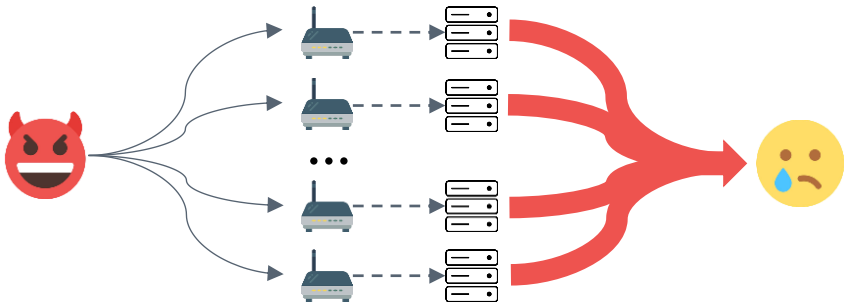
Mitigation by Network Ingress Filtering



Networks with transparent forwarders do not follow **BCP38** as they allow spoofed traffic to pass through the network.

Solution. Implement network ingress filtering; ensuring that only traffic from allowed ranges passes through.

Mitigation by Strict Rate Limiting



Local rate limiting. Public DNS providers should strictly limit DNS replies, e.g., by limiting the number of queries per second.

Global rate limiting. Anycast public DNS providers should always implement a global monitoring strategy to detect anomalies.

Conclusion

Transparent forwarders are a serious threat to the public Internet.

1. Transparent forwarders are **misconfigured devices**

We update our dataset regularly and make it publicly available.

https://odns-data.netd.cs.tu-dresden.de

Conclusion

Transparent forwarders are a serious threat to the public Internet.

1. Transparent forwarders are **misconfigured devices**
2. Transparent forwarders allow for significantly **higher attack traffic**

We update our dataset regularly and make it publicly available.

https://odns-data.netd.cs.tu-dresden.de

Conclusion

Transparent forwarders are a serious threat to the public Internet.

1. Transparent forwarders are **misconfigured devices**
2. Transparent forwarders allow for significantly **higher attack traffic**
3. Transparent forwarders can be orchestrated to **circumvent local rate limiting**

We update our dataset regularly and make it publicly available.

https://odns-data.netd.cs.tu-dresden.de

Conclusion

Transparent forwarders are a serious threat to the public Internet.

1. Transparent forwarders are **misconfigured devices**
2. Transparent forwarders allow for significantly **higher attack traffic**
3. Transparent forwarders can be orchestrated to **circumvent local rate limiting**
4. Transparent forwarders allow to **bypass shielded resolvers**

We update our dataset regularly and make it publicly available.

https://odns-data.netd.cs.tu-dresden.de

Conclusion

Transparent forwarders are a serious threat to the public Internet.

1. Transparent forwarders are **misconfigured devices**
2. Transparent forwarders allow for significantly **higher attack traffic**
3. Transparent forwarders can be orchestrated to **circumvent local rate limiting**
4. Transparent forwarders allow to **bypass shielded resolvers**
5. Eliminating the impact of transparent forwarders **requires little changes**

We update our dataset regularly and make it publicly available.

https://odns-data.netd.cs.tu-dresden.de