CIRCL
Computer Incident
Response Center
Luxembourg

DDoS and Attribution: Observations of Attacks against North Korea

The Void - An interesting place for network security monitoring

Alexandre Dulaunoy

2017-11-15 Luxembourg Internet Days

CIRCL - Computer Incident Response Center Luxembourg

Who we are

CIRCL
Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.
- CIRCL leads the development of **MISP, an open source threat intelligence platform** to support information sharing and analysis in cyber security.
- We also operate a honeypot sensor network on **unused address spaces**.

The infinite value of crap

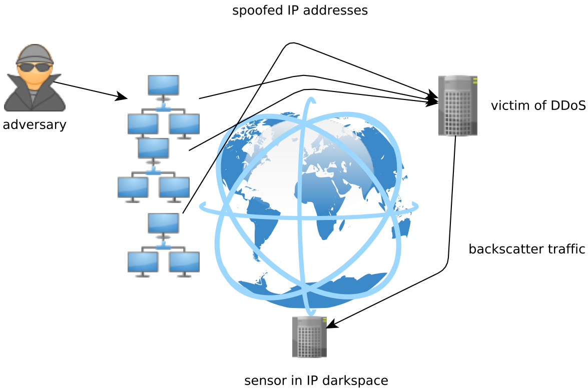
The Internet is noise

from a series of packets hitting our darkspace

Motivation and background

- IP darkspace or black hole is
  - **Routable non-used address space** of an ISP (Internet Service Provider),
  - incoming traffic is unidirectional
  - and **unsolicited**.
- Is there any traffic in those darkspaces?
- If yes, what and why does it arrive there?
  - And **on purpose** or **by mischance**?
- What's the security impact?
- Can we find victims and potential attackers by monitoring noise?

Monitoring DDoS activity from internet backscatter



Internet backscatter and DDoS targeting North Korea

- North Korea has a minimal topology which provides a baseline for backscatter traffic analysis.
- BGP connectivity of North Korea is low compared to other countries (one upstream provider who recently changed from CN to RU) and not very diversified allowing a **passive network enumerations**.
- Tactical and political information often published and largely disseminated in advance (e.g. recent US Cyber Command statement about DDoS against North Korea).

Overview of major DDoS in 2017 against North Korea

Table 1: 2017 backscatter observed from AS131279 (Star JV)

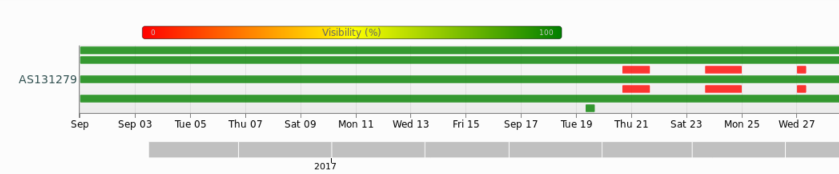
2017-03-11	TCP/80 DDoS
2017-03-13/16	TCP/80 and TCP/53 DDoS
2017-03-28	TCP/80 DDoS⋆
2017-05-04	TCP/80 DDoS
2017-08-08	TCP/80 DDoS
2017-09-13/16	TCP/80 and TCP/53 DDoS↑∗
2017-09-22/25	TCP/80 and TCP/53 DDoS↑◇
2017-09-26	TCP/80 DDoS
2017-10-04	TCP/80 DDoS

⋆ North korea test-fired a KN-17 ballistic missile ∗ North Korea launched a ballistic missile on September 15 from Sunan airfield

◇ (US) Executive Order 13810 - Imposing Additional Sanctions with Respect to North Korea.

Conclusion

- Passive analysis from backscatter can **confirm BGP instability** due to DDoS attacks (cf. AS1311279 in September):



- Discovering **new techniques, trends, adversaries or victims** can be done with backscatter analysis.
- Interested to gather noise from unused network space or share threat intelligence? Contact us at `https://www.circl.lu/`.

References

- *Zalewski M.* Silence on the wire: a field guide to passive reconnaissance and indirect attacks. No Starch Press; 2005.
- *Team CIRCL* Darknet and Black Hole Monitoring a Journey into Typographic Error. Honeynet Project Workship; 2014.
- *Team CIRCL, Restena CSIRT* An Extended Analysis Of An IoT Malware from a Blackhole Network. TNC17 Networking Conference; 2017.