Review of

Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope

By Raphael Hiesgen, Marcin Nawrocki, Alistair King, Alberto Dainotti, Thomas C. Schmidt, Matthias Wählisch

What is the problem?

Large-scale Internet scans are a common method to identify victims of a specific attack. Host scanning is instrumental to discover vulnerable services, create botnets, and launch cyberattacks- example the Mirai botnet. Stateless scanning like in ZMap has been established as an efficient approach to probing at Internet scale. Stateless scans, however, need a second phase to perform the attack. This remains invisible to network telescopes, which only capture the first incoming packet, and is not observed as a related event by honeypots, either. A solution is needed

Summary

In this work, we examine Internet-wide scan traffic through Spoki, a reactive network telescope operating in real-time. Spoki responds to asynchronous TCP SYN packets and engages in TCP handshakes initiated in the second phase of two-phase scans. We analyse two-phase scanners during a three month period using globally deployed Spoki reactive telescopes as well as flow data sets from IXPs and ISPs. We find that a predominant fraction of TCP SYNs on the Internet has irregular characteristics. Our findings also provide a clear signature of today's scans as: (i) highly targeted, (ii) scanning activities notably vary between regional vantage points, and (iii) a significant share originates from malicious sources

Key Insights

1. Independently of the exploited protocol and vulnerability, two-phase scans act as a catalyst. To protect against two-phase reconnaissance scans, we encourage network operators to deploy alert or filter rules, while scanning for research purposes could be accepted.

2. System maintainers should be aware that their vulnerable devices can be discovered within hours and any exploit may turn their systems into an active scanner. They should monitorfor malicious activities and shorten update cycles

3. Developers of monitoring tools should support software that reacts to irregular TCP SYNs even though those SYNs do not comply with common TCP behavior, otherwise users of monitoring systems, including operators and researchers, will see fewer types of attacks

Strengths

1. Spoki: A Reactive Network Telescope that answers TCP SYNs in real time
2. One Spoki component is able to handle about 250,000 packets per second. This scales linearly, and 1Mpp can be handled by only four components.
3. They deploy Spoki in four /24 IP prefixes across the US and Europe on **commodity hardware.**
4. They provide source code and detailed build guide for building and running spooki
5. Entire research is very data driven.

Summary of Key Results

1. Today's scans are: (i) highly targeted, (ii) scanning activities notably vary between regional vantage points, and (iii) a significant share originates from malicious sources
2. stateless SYN scanning contributes more than two-thirds of TCP SYN traffic

Open Questions?

Will the developers and maintainers pay attention to recommendations made in this paper to make systems probe resistant?