"rucki zucki" scanning tool

"rucki zucki" scanning tool

João Collier de Mendonça @joaocmendonca1
Andreas Petker @mansior

why

CERTs must frequently evaluate emerging issues

- problems on own infra/customer devices
- heartbleed (apr. 2014)
- shellshock (sep. 2014)
- house-of-keys (nov. 2015)
- hardware backdoors `FGTAbc11*xy+Qqz27`, `<<< %s(un='%s') = %u`, ...
- tls drown (Mar. 2016) || sslv2 related issues

and still be **very fast**

main challenge

tools and processes must cope with
a large™ number of IP addresses

large ~ 20^9

Customers	Germany (Millions)	Group (Millions)
Mobile	40	156
Fixed	20	29
Broadband	12	17.8

motivation

why did we have to build our own solution?

- reactive nature of a CERT's duties
  →| once triggered, no time to lose
- be able to get a clear assessment asap
- avoid waiting for PoC scripts (or MSF Modules)

motivation (2)

why scan if your have shodan.io/censys.io?

- shodan $/€
- lack of transparency (*how* & *when*)
- no data for internal/non-routable addresses
- shodan/censys data are not as accurate as we need, eg. no info on static/dynamic/mobile address pools.

own tools provide more detailed and up-to-date results than publicly-available data

how does this work?

stage 1: bazooka mode

Image source: IWM (NA 8376), iwm.org.uk

stage 1: masscan

- started with own tools and script (no good)
- masscan is the tool of choice for large-scale scans
- very quickly find possibly affected hosts (fast triage)
- output results for post-processing (stage 2)

stage 1: masscan performance

resource	hosts/sec (tcp)	hosts/sec (udp)
vServer (1Gbps link, 2x1,6GHz, 4GB)	144 kpps	109~400 kpps

- Usual rates with modest resources > 100kpps
- Important: scan from outside your AS (external view)

stage 2: sniper mode

Image source: IWM (B 8179), iwm.org.uk

stage 2: detailed scan

- second-stage tool is typically either a self-written script or public proof-of-concept
- takes results from first stage and does in-depth checks
- ~10-100x slower than first stage

what is "rucki zucki"?

what is "rucki zucki"?

- "rucki zucki" connects both stages (bazooka, sniper)
-  "wrapper" script that controls masscan and a second-stage tool
- second-stage tool is typically either a self-written script or public proof-of-concept

functionalities and config options

- retrieve IP subnets/ranges (RIPE REST API) for specified AS
- parses subnet values and executes masscan/scripts
- logging, validation checks
- configuration options for both stages
- easy-integration of scripts, nmap scripts, python etc

Q&A

#thankyou

Andreas Petker @mansior
João Collier de Mendonça @joaocmendonca1

Q&A

Q&A

- how does "rucki zucki" handles parallelization?
- what second stage modules did you develop so far?
- for which assessments did you use it so far?

speakers' bios

Andreas Petker @mansior

Andreas is a Security Analyst at Deutsche Telekom Cyber Defense Center since 2009. He is mainly focused on Vulnerability and Advisory Management and rapid prototyping of incident detection and response tools.

João Collier de Mendonça @joaocmendonca1

João is an Incident Handler/Security Analyst at Deutsche Telekom Cyber Defense Center since 2010. He is mainly focused on network-based incident detection and build-up of incident handling know-how across Deutsche Telekom Group.