South African NREN CSIRT Update

17 September 2019

Roderick Mooi
CSIRT Information Security

SANREN CSIRT update
Roderick Mooi, SANREN, TENET SLARG 2018

watching/stealing/abusing

Malware

DDoS

Exploit platform

IP theft

CSIRT Services
SA NREN CSIRT History

- 2012: Started asking what we do (and should do) re malicious activity
- 2015: Workshop with community representatives
- 2016: Launched the CSIRT
- 2017: Listed with TI
- Nov 2018: Accredited with TI
- 2019: FIRST fellowship → membership
Services

• Incident response support and coordination
  Email: csirt@tenet.ac.za

• Vulnerability assessments
  https://csirt.sanren.ac.za/services_vulnscan.html

• Articles
  https://csirt.sanren.ac.za/categories/cat_announcement.html

• Securing SA NREN Infrastructure
In development: Alerting Service

- **Input**
  - Feeds from global scanning systems
  - Flow analysis
  - Honeypots

- **Processing**
  - Correlation to malicious events
  - Correlation to system owner

- **Output**
  - Email alerts / portal
**Description of Host Infected with Malware**

- **Port**: 4433
- **City**: CAPE TOWN
- **Description**: This host is most likely infected with malware.
- **Destination Domain Name**: disorderstatus.ru
- **Destination CC**: US
- **Destination IP**: 72.5.161.4
- **Destination Port**: 80
- **Malware Family**: avalanche-andromeda
- **Source**: Bitsight
- **Source Time**: 2019-08-19 00:01:52Z
- **Report Type**: botnet_drone
- **Feeder**: shadowserver
- **Feed**: botnet drone

**Description of Host Running Publicly Accessible SMB Service**

- **Port**: 445
- **City**: CAPE TOWN
- **Description**: This host is most likely running a publicly accessible SMB service, which can be accessed through Open SMB.
- **Reverse DNS**: [Redacted]
- **Source Time**: 2019-08-18 11:38:17Z
- **Feeder**: shadowserver
- **Feed**: smb scanning project
- **Type**: vulnerable service
- **IP**: [Redacted]
- **CC**: ZA
2018 Survey

- 22 respondents

- ~25% experienced a major incident (past year)
  Ransomware (x4), cryptocurrency mining and phishing
Trend: Increasing Activity

Spam (unfiltered) @ 86%!
Cyber Security Challenge
by NRENs, for students...

- Information security related contest
- Capture the flag / token
  (jeopardy-style challenges)
- Hacking web, mobile, cryptography, IoT,
  reverse engineering, forensics...
- Attack & defend

Aimed at students/hobbyists \(\Rightarrow\) new talent

“Every team had their own server with certain vulnerabilities placed by the Hacking-Lab staff. On the one hand everyone had to defend their own server and services against attacks from the opposing teams and on the other hand the teams had to patch vulnerabilities, achieve, decipher, solve, attack, defend, patch, sustain, poown.

Interested?
csc@sanren.ac.za

“9.2. Goal
Join your laptop to the robot WiFi network. Hijack the robot controller. Navigate the robot to the jury, and make it play a sound file which tells the team name.”
TRANSITS I 2018 + again Dec 2019
Thanks!
roderick@sanren.ac.za
csirt@sanren.ac.za