Open Source Intelligence Aggregation

TF-CSIRT      MAY 15TH, 2017

Rogier Spoor
Sjors Haanen
Why?

• Nowadays a working IT infrastructure is critical
• Services are interconnected and reachable
• Security often not on par:
  - Bugs in outdated software;
  - Wrong configuration;
  - Default/weak passwords;
  - Password reuse.
After MongoDB attack, ransomware groups hit exposed Elasticsearch clusters

Over 600 Elasticsearch instances had their data wiped and replaced with a ransom message.
What does the outside world know about us?
Lots of vulnerabilities are like low hanging fruit
Problem

- Missing aggregation of Open Source Security Intelligence (OSINT)
  - Missing overview;
  - False positives;
  - Awareness of exploitable vulnerabilities;
  - The bad guys are often quicker.
Goals

- Give CSIRTS insights in vulnerabilities/services exposed to the world;
- Let users share and discuss search queries to make it a collaborate project;
- Reducing the cyber crime possibilities;
- Reducing the time to "fix";
- Doing the right things (focus on high risk).
Workings of IOT-scanner

1. Scan device for services
2. Store service banners
3. End users can search on banners
Source: IOT-scanners
Source: IpInfo

REMCO VERHOEF
Founder of Honeycast.io
@remco_verhoef hackerone

- Enriching found data about IP-addresses
- Online blacklists

IpInfo

geolite

check.torproject.org

whois

Real-time Blackhole Lists

11/16
Proof of Concept
Collaboration with GDI Foundation

Tool is used at GDI Foundation
Scope: worldwide

GDI.Foundation
A safer Internet for everybody & everywhere

Project “Internet & Cyber Security Health Check”

Victor Gevers
@0xDUDE

Vincent Toms
(IT) Security Specialist & co-founder GDI.Foundation
The Hague Area, Netherlands | Information Technology and Services
Future:
• Additional OSINT sources
• GDI: upscale
Demo

- Visualisations with Kibana
- Datasets:
  - as-surfnet (123K IPs);
  - GDI: Dahua IP cameras