How to Spot the Blue Team?

Red Team Infrastructure Security

R.A.H. Lahaye
Supervisors:
Marc Smeets and Mark Bergman
Outflank

Research Project 2

System and Network Engineering
University of Amsterdam

February 5, 2018

Outline

Introduction

- Red Teaming vs Blue Teaming
- Team Goals

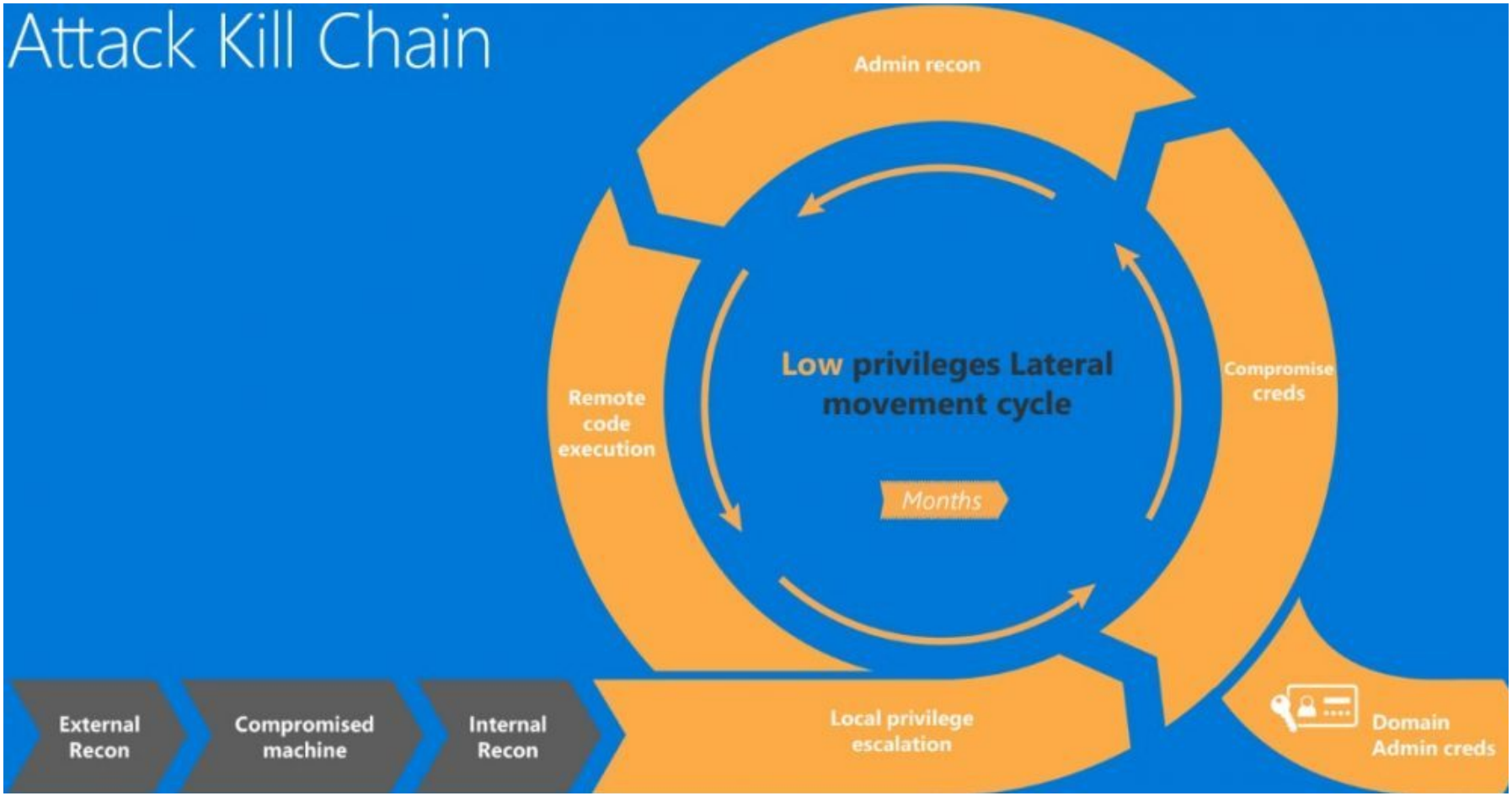

Figure: Red Team Kill Chain[mic, 2016]

Project Goal

- Find a way to detect blue team **actions** so that the red team can stay undetected and achieve long-term engagement.
- Project is **not** about how to stay undetected as a Red Team

Research Question

1. How to secure a red team infrastructure to detect a blue team analysis?
    1. How does a red team infrastructure look like?
    2. How can a blue team analysis be detected?

Related Work

- No related work regarding detecting a blue team analysis
- Some related work regarding how a red team operation and infrastructure looks:
  - Wiki to collect Red Team infrastructure hardening resources[Dimmock]
  - Cobalt Strike - Red Team Operations Course and Notes[cob, 2013]
  - Powershell Empire - Documentation[pow]

Method

- Literature Study and interviews to figure out how a typical red team infrastructure look like
- Analysis of a red team operation software to know how an operation looks like
  - Cobalt Strike
  - PowerShell Empire
- If you know what a Remote Access Tool's request looks like, you know what legit traffic/events are, and what not

Red Team Infrastructure

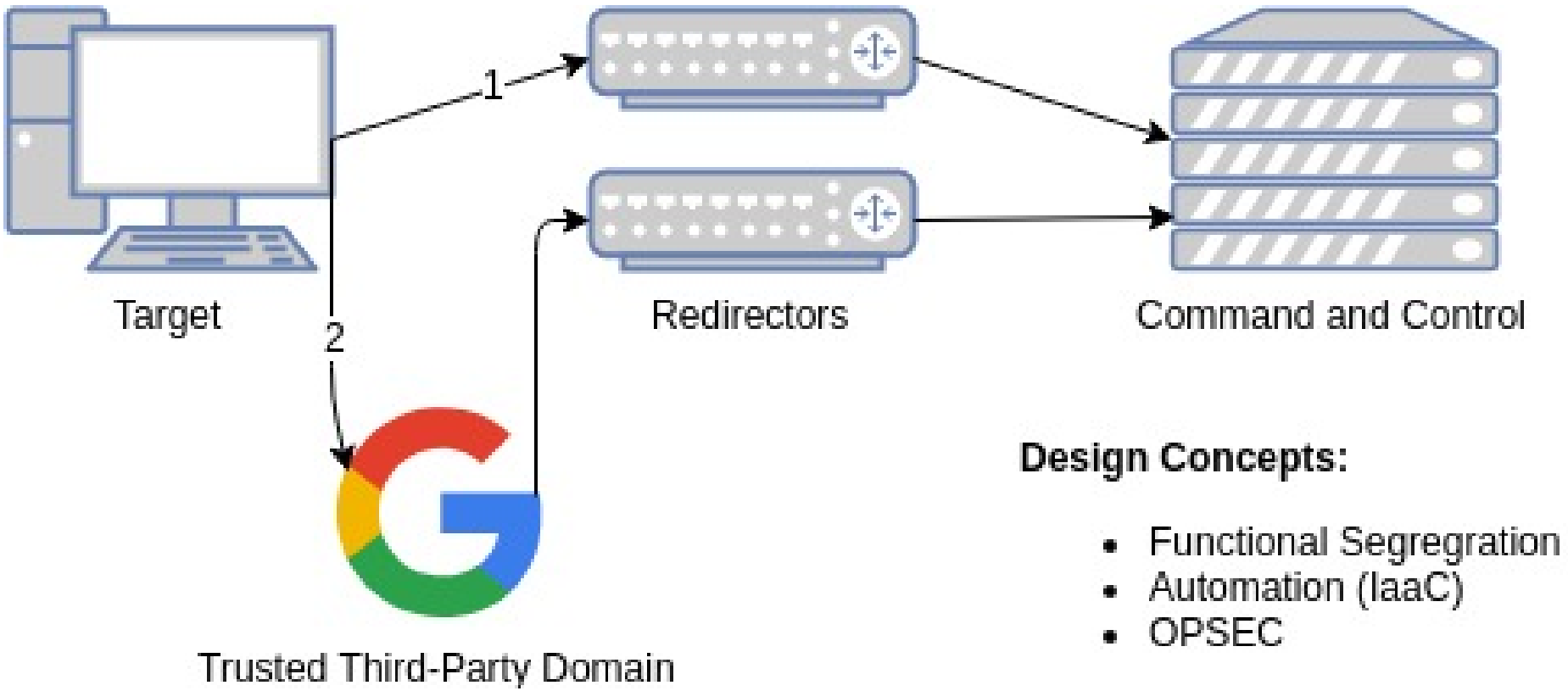

Figure: Red Team Infrastructure

Red Team Infrastructure Security

Desired Security Controls

- Preventive Security Controls (Limited)
  - Firewall
  - System Hardening
  - Concealment
- Detective Security Controls
  - Logging and Monitoring
  - IDS
- Responsive Security Controls
  - Disposing/New Infrastructure
  - Distraction/Decoy

Proof of Concept

Requirements:

- Able to detect a Blue Team's analysis of a Red Team's operation
- Usable for multiple Red Team operations
- Should not trigger by random Internet scans

Infrastructure

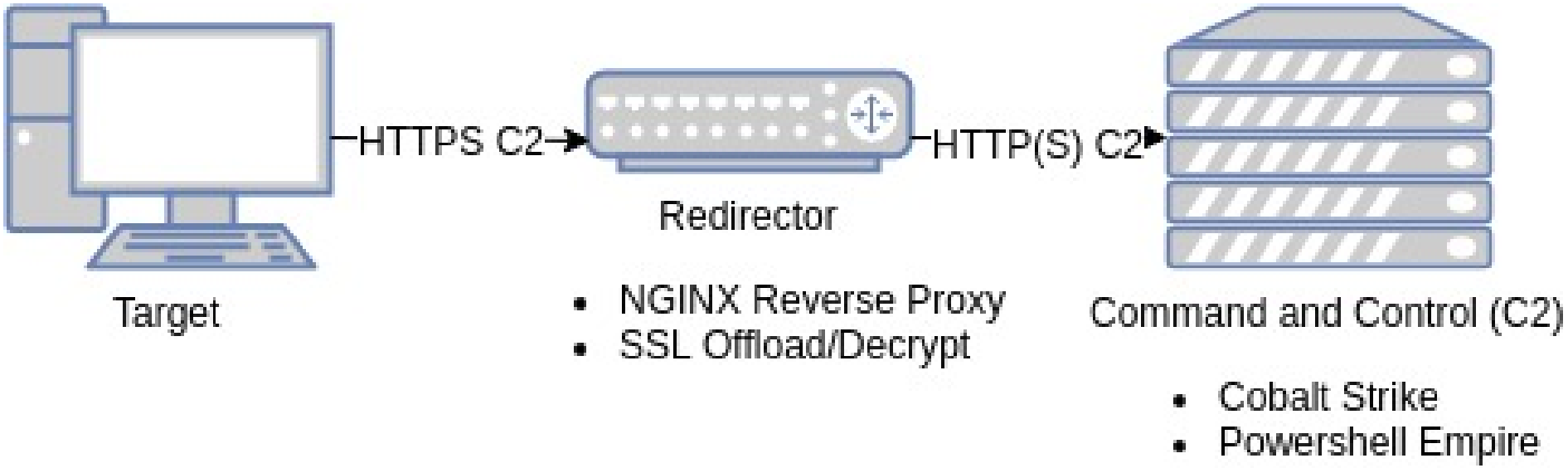

Figure: Proof of Concept Basic Red Team Infrastructure

Red Team Software Analysis

- Focused on successful callback and communication from target
- HTTP/(S) Requests for communication (or other protocols)
- DNS Domain Lookups

How to Spot the Blue Team?

HTTP(S) Communication Paths

Command and Control Communication Paths:

- "/legit/communication/uri/to/filter/with/get.php"
- "/legit/communication/uri/to/filter/with/news.php"
- "/legit/communication/uri/to/filter/with/login/process.php"

Blue Team:

- "/legit/communication/uri/to/filter/with/"
- "/legit/communication/uri/to"

Anomaly:

- No fully complete Command and Control communication path
- Contains first prefix ("/legit/*")

User-Agents

Command and Control User-Agent:

- "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"

Blue Team:

- "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36"

Anomaly:

- Different User-Agent compared to the Command and Control User-Agent

GEO Location

Target Location:

- Country: Netherlands

Blue Team:

- Country: Russia

Anomaly:

- Command and Control traffic from unexpected location

DNS Domain Lookup

Command and Control Lookup:

- "rt-1.very.legit.domain.tours.prac.os3.nl"

Blue Team:

- "domain.tours.prac.os3.nl"
- "very.legit.domain.tours.prac.os3.nl"

Anomaly:

- Any other sub-domain lookup

Virustotal

Command and Control Beacon/Payload:

- Known Hash

Blue Team:

- Upload to Virustotal

Anomaly:

- When hash is known by Virustotal while the Red Team uses unique files

Logging Infrastructure

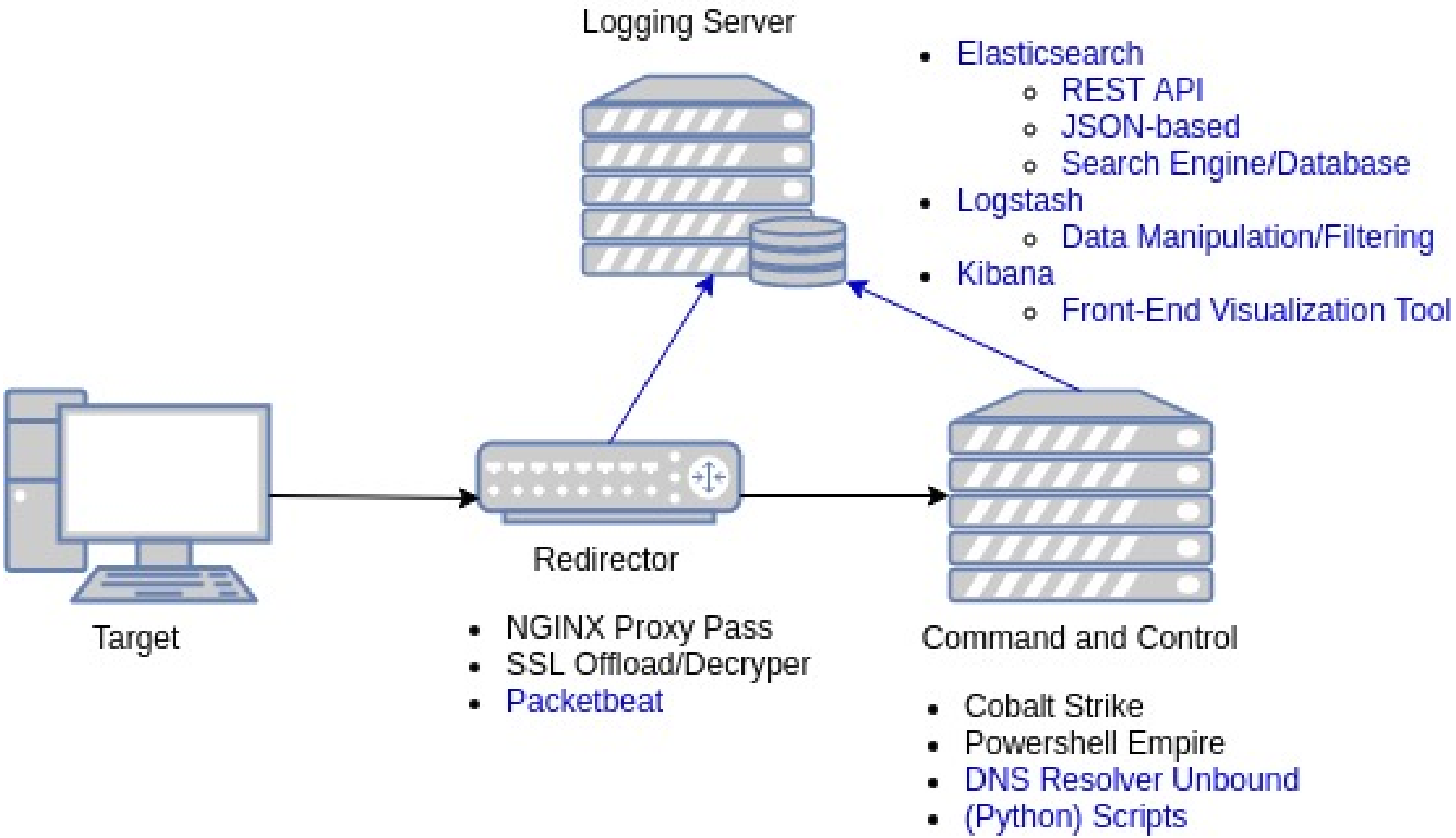

Figure: Proof of Concept Logging Infrastructure

Proof of Concept Advantages and Disadvantages

Advantages:

- API
- Good for logging data

Disadvantages:

- Complex
- Not good for events/alerts (nor with other alternatives)
- Hard to find needed data (especially with multiple Red Team operations)

Better alternatives?

Usage: query.py [options]

```
ricklahaye@Sioux-Falls:~/red-team-infrastructure-security/python$ ./query.py --help
Usage: query.py [options]

Options:
  -h, --help            show this help message and exit
  --host=HOST           host [10.0.0.1]
  --port=PORT           port [9200]
  --paths=PATH          C2 paths [/legit/communication/uri/to/filter/width/get
                        .php,/legit/communication/uri/to/filter/width/news.php
                        ,/legit/communication/uri/to/filter/width/login/proces
                        s.php]
  --user_agent=USER_AGENT
                        C2 user agent [Mozilla/5.0 (Windows NT 6.1; WOW64;
                        Trident/7.0; rv:11.0) like Gecko]
  --index=INDEX         index [packetbeat-*]
  --geo-country=GEO     country [Netherlands]
  --dns=DNS             dns host name
                        [rt-1.very.legit.domain.tours.prac.os3.nl]
  --dns-prefix=DNS_PREFIX
                        dns host name prefix root [*domain.tours.prac.os3.nl]
ricklahaye@Sioux-Falls:~/red-team-infrastructure-security/python$
```

Figure: query.py options

query.py output

```
ricklahaye@Sioux-Falls:~/red-team-infrastructure-security/python$ ./query.py
<bound method Elasticsearch.info of <Elasticsearch([{'host': '10.0.0.1', 'port': '9200'}])>>
* User Agent
- Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
- Paths: ['/legit/communication/uri/to/filter/width/get.php', '/legit/communication/uri/to/filter/width/
news.php', '/legit/communication/uri/to/filter/width/login/process.php']
- Status: 6 anomalies
* Geo Location
- Geo Country: Netherlands
- Paths: ['/legit/communication/uri/to/filter/width/get.php', '/legit/communication/uri/to/filter/width/
news.php', '/legit/communication/uri/to/filter/width/login/process.php']
- Status: No anomalies
* Virustotal
- Status: 9 anomalies
* Communication Paths
- Paths: ['/legit/communication/uri/to/filter/width/get.php', '/legit/communication/uri/to/filter/width/
news.php', '/legit/communication/uri/to/filter/width/login/process.php']
- Status: 42 anomalies
* DNS
- DNS: rt-1.very.legit.domain.tours.prac.os3.nl
- DNS Prefix: *domain.tours.prac.os3.nl
- Status: 41 anomalies
ricklahaye@Sioux-Falls:~/red-team-infrastructure-security/python$
```

Figure: query.py output

Conclusion

- Typical Red Team infrastructure uses redirectors and Command and Control servers that are disposable and automated
- Detecting the Blue Team requires knowledge of own Red Team's operation and its used tools
- Detecting the Blue Team can be done with a monitoring and logging infrastructure
- No good tooling is available to detect the Blue Team

Future Work

- Build free and working plugin for Kibana for alerting
- Improve the Python script's output
- Create a tooling that is able to learn a Red Team operation
- Many others..

Questions

Are there any questions?

References

Powershell empire documentation. URL https://www.powershellempire.com/?page_id=83.

Cobalt strike red team operations course and notes, 2013. URL https://blog.cobaltstrike.com/2013/10/18/tradecraft-red-team-operations-course-and-notes/.

Disrupting the kill chain, 2016. URL https://cloudblogs.microsoft.com/microsoftsecure/2016/11/28/disrupting-the-kill-chain/.

J. Dimmock. Wiki to collect red team infrastructure hardening resources. URL https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki.