Normalizing Empire's Traffic to Evade Anomaly-Based IDS

Utku Sen - Gözde Sinturk
Whoami

- Working @ Tear Security
- utkusen.com
- twitter.com/utkusen
Outline

- Current state of defense and assume breach scenarios
- Signature/Anomaly based NIDS and evasion
- A brief information about Empire project
- Anomaly based NIDS and Empire
- Proposed solutions
- firstorder tool
A Basic Network

Perimeter Defenses (Firewall)

NIDS (Network Intrusion Detection System)

Clients

Some Other Assets
A Basic Network
NIDS (Network Intrusion Detection System)

- Signature-Based
- Anomaly-Based
Signature-based NIDS

- Looks for pre-defined patterns of previously known attacks.
- Doesn’t require a training phase.
- Highly available and popular.
- Can’t catch zero-day/new attacks.
Evasion

- Not complex but not super easy.
- Change traffic elements.
- Don’t match with any signatures.
Anomaly based NIDS

• Builds a statistical model describing the normal network traffic, and flagging the abnormal traffic.

• Requires training phase.

• Uses math, machine-learning and various sophisticated thing.

• Expensive $$$

• Might catch zero-day/new attacks.
Anomaly based NIDS

Recorded Daily Traffic
- SMTP - mail.acme.com/ Subject: Meeting notes
- HTTPS - youtube.com/ (8 hours active traffic)
- SSH - development.acme.com

New Traffic
POST /read.php HTTP/1.1
Cookie: session=VAGyTO1KBPO0BxJ45BZrcm3BinQ
{"Utku Sen":"122-124-12424"}

LEARNING ALGORITHM
PATTERN (NORMAL TRAFFIC PROFILE)
NORMAL
ANORMAL
Evasion

- Pre-training
- Post-training
Pre-Training Evasion

- Generate malicious traffic on the network.
- Algorithm will accept it as regular network traffic.
“It’s not realistic.”

—Anyone
A Realistic Scenario?

- Anomaly-detection engine is trained by *real* regular traffic.
- Watches the whole network.
- Attacker should gain a foothold on the network and exfiltrate data without causing any anomaly alert.
Empire

Listener (C&C Server) - Command - Agent

Output
Key Traits of HTTP Listener

- **KillDate**: Date for the listener to exit
- **DefaultDelay**: Agent delay/reach back interval
- **WorkingHours**: Hours for the agent to operate
- **DefaultProfile**: User-agent value and URI specification for the agent
- **DefaultJitter**: Jitter in agent reachback interval
- **Port**: Listening port of the C2 server
- **StagingKey**: Staging key for initial agent negotiation
- **ServerVersion**: Server header for the C2 server.
C2-Agent Communication

- "Client Data" is symmetrically encrypted with AES algorithm where encryption key is client’s session key.

- "Metadata/Routing Data" is symmetrically encrypted with RC4 algorithm where encryption key is "StagingKey" of the listener.

Command: whoami

Response: root
NIDS on Empire’s HTTP Listener

- Request URI
- User-agent value
- Server header
- Default HTML Content
- Port
- Connection Interval (DefaultDelay)

```
GET /read.php HTTP/1.1
Cookie: session=VAGyT01KBPOOBxJ45BZrcm3BnQ
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
            Chrome/41.0.2228.0 Safari/537.36
Host: 192.168.1.26
Connection: close
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 208
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Server: Microsoft-IIS/7.5
Date: Thu, 08 Feb 2018 17:57:40 GMT

<html><body><h1>It works!</h1><p>This is the default web page for this server.</p><p>The web server software is running but no content has been added.</p></body></html>
```
NIDS on Empire’s HTTP Listener

• Post Request Body
Traits

- Can be Changed in Options Menu
  - Request URI
  - User-agent value
  - Server header
  - Port
  - Connection interval

- Requires Source Code Change
  - Default HTML content
  - POST request body
Proposed Solution

• Polymorphic Blending Attack (PBA): Creating attack packets which are matches to normal traffic profile

I have to learn what is considered as normal

Let’s capture the traffic and check what’s inside
Steps For The First Group of Traits

- Get traffic capture data of a normal traffic and define normal behaviour of users. (Request URI, User-agent, Server header, Port)

- Change Empire’s listener traits according to first step.

- Start the C2-agent communication.
Adjusting The Connection Interval

- False-positive rate of an anomaly detection system has a positive correlation with the size of the network.
- More computers = less connection interval
- Less computers = more connection interval
- More connection interval is better in most cases.
Steps For The Second Group of Traits

- Get traffic capture data of a normal traffic and define normal behaviour of users. (Default HTML Content)

- Change Empire’s listener traits according to first step.

- Start the C2-agent communication.
Post Request Body

**ENCRYPTED**

Command: whoami ➔ *+1kJas82=½$5 ➔ Laptop ➔ %'^'Aj8&a=283. ➔ Response: root

**Plain Text**

Command: whoami ➔ Laptop ➔ Response: root

**Real Sh*t?**

**I sleep**

**Anomaly-based**

**Signature-based**

**Real Sh*t?**
Markov Obfuscation

- Published by Cylance SPEAR Team (https://github.com/CylanceSPEAR/MarkovObfuscate)
utku-MacBook-Pro:MarkovObfuscate utku$ cat passwd.txt
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
_installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false
_lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
utku-MacBook-Pro:MarkovObfuscate utku$
chapter v. the prisoner pass. the door were there was. one of his son in the prisoner with you. i hope. the door of his. the bank. the. that he could and. and when he could justly. the. have been so dear. the. we have. a. i thank you. he left. the. their. and put to the door when no. i would have been to the prisoner before their. and my dear to. on the door tenderly kissed her. and women. the door who at the prisoner on. at the door carefully feeling confident if you. that he could bear it was a matter of the doctor play. the door where the. he thought of the door like spray. the door belonged through about. the doctor occupied with a long which he was over the. and which he was a. and they were. yes. the prisoner to you. and you. and one of a strong and. i trust my dear to the doctor manette to let me. and at the prisoner could endure. the doctor disquieted. the doctor entreated her. he bent over the. and even to the. defarge. he felt it was the guard. the. they were not leave the. i was a. as he was no. and which he was as he had fallen on the. they were. how. the. your. he at the prisoner in general. the doctor repeated the. the day. the courtyard. the prisoner looked. the prisoner with dust and. he were. i want to the. as he was very. and many. and what is a prison of the doctor. the. all the. defarge. i come to the. he had. be. i say. the door again mr. the. then. i see the. and which he could endure. the doctor occupied with a long life. the doctor shaded his. i would have been dragged out of the courtyard. the door where dire exasperation. the. good. the fire. the. at the door the door. the doctor communicated. the prisoner of death. the. mr. the doctor distinctly in the doctor had been the young lady. the room. the. darnay. he knows. the. have been so strong and. and was a. this. and would have no no. the rest. the door to him. and her. and their. and when he could or. the best of the door and a. and
Operation Steps

• Encode Empire’s encrypted data with Base64 to get rid of non-printable characters.

• Download the dataset from an external source.

• Train the encoded data with dataset.

• Send Markov encoded data with dataset to C2 server.
Anomaly Based IDS

Attacker

encoded payload + dataset

I sleep

Local Network

Agent deployed

encoded payload + dataset

Get lots of English texts

dailynews.com
Drawbacks

- Data training will consume time and resource.
- You need to implement the Markov Obfuscation code inside the agent.
firstorder Tool

- Extracts valuable information from a PCAP file and configures Empire’s listener.

- Most used ports, URI, server headers, user-agents, number of machines etc.

- Configures Empire’s listener automatically.
Empire

265 modules currently loaded
0 listeners currently active
0 agents currently active
(Empire) >
Conclusions

- Defense mechanisms are getting smarter.
- Attackers should create smarter methods which can mislead an AI.