Existing Work

Here is where we should save all of our existing links

https://www.slideshare.net/ChrisRoberts197/artificial-intelligence-in-infosec

Ice In *Neuromancer* by Gibson

ICE

Intrusion Countermeasures Electronics

http://williamgibson.wikia.com/wiki/Intrusion_Countermeasures_Electronics

The Dixie Flatline and AI Ice

`Just thinking out loud... How smart's an AI, Case?'

`Depends. Some aren't much smarter than dogs. Pets. Cost a fortune anyway. The real smart ones are as smart as the Turing heat is willing to let 'em get.'

`Look, you're a cowboy. How come you aren't just flat- out fascinated with those things?'

`Well,' he said, `for starts, they're rare. Most of them are military, the bright ones, and we can't crack the ice. That's where ice all comes from, you know? And then there's theTuring cops, and that's bad heat.' He looked at her. `I dunno, it just isn't part of the trip.'

“How'd you know it was an AI?'

`How'd I know? Jesus. It was the densest ice I'd ever seen. So what else was it? The military down there don't have any-thing like that. Anyway, I jacked out and told my computer to look it up.'

`Yeah?'

`It was on the Turing Registry. AI. Frog company owned its Rio mainframe.'

Case chewed his lower lip and gazed out across the plateaus of the Eastern Seaboard Fission Authority, into the infinite neuroelectronic void of the matrix. `Tessier-Ashpool, Dixie?'

`Tessier, yeah.'

`And you went back?'

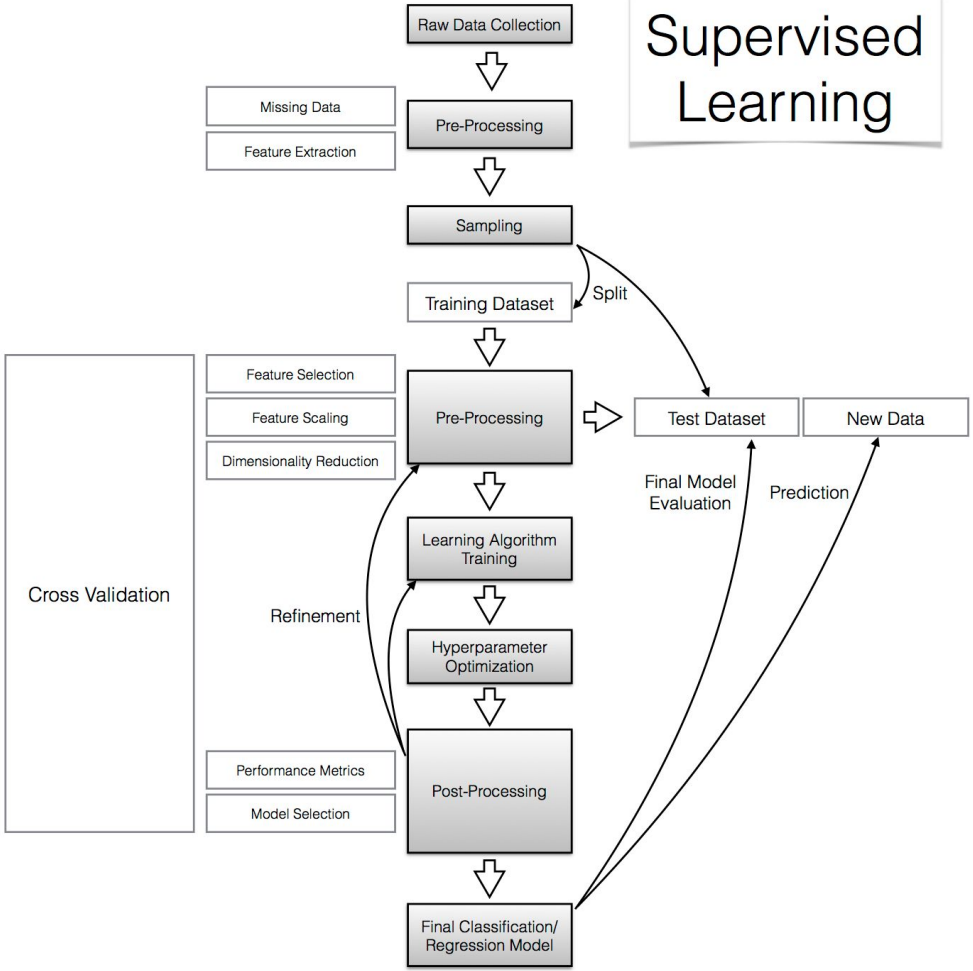
`Sure. I was crazy. Figured I'd try to cut it. Hit the first strata and that's all she wrote. My joeboy smelled the skin frying and pulled the trodes off me. Mean shit, that ice.'

`And your EEG was flat.'

`Well, that's the stuff of legend, ain't it?'

Case jacked out. `Shit,' he said, `how do you think Dixie got himself flatlined, huh? Trying to buzz an AI. Great...'”

Supervised Learning



MIT’s AI2

https://news.ycombinator.com/item?id=12037474

Fuck these guys for doing the exact methodology I planned on doing.

Luckily, what they studied nothing like what we are going to do.

They went after behavior, which is dumb.

We go after traffic. Human augmented is the move though.

Fuckers.

Human Augmented Training

Video:

https://youtu.be/b6Hf1O_vpwQ

Article:

https://www.fastcodesign.com/3058908/artificial-intelligences-ultimate-challenge-cyber-terrorism

Paper:

https://people.csail.mit.edu/kalyan/AI2_Paper.pdf

How It Works

We present an analyst-in-the-loop security system, where analyst intuition is put together with stateof-the-art machine learning to build an end-to-end active learning system. The system has four key features:

- a big data behavioral analytics platform
- an ensemble of outlier detection methods
- a mechanism to obtain feedback from security analysts
- a supervised learning module.

Existing Models

Existing Models

Slingbot

TAMD

BotGAD

BotMiner

SBotMiner

BotSniffer

BotHunter

AutoRE

https://link.springer.com/chapter/10.1007/978-3-642-17610-4_26#page-2 - decent overview

Academic Papers

BotFinder: Finding Bots in Network Traffic Without Deep Packet Inspection

In this paper, we present BOTFINDER, a novel system that detects infected hosts in a network using only high-level properties of the bot's network traffic. BOTFINDER does not rely on content analysis. Instead, it uses machine learning to identify the key features of command-and-control communication, based on observing traffic that bots produce in a controlled environment. Using these features, BOTFINDER creates models that can be deployed at network egress points to identify infected hosts. We trained our system on a number of representative bot families, and we evaluated BOTFINDER on real-world traffic datasets – most notably, the NetFlow information of a large ISP that contains more than 25 billion flows. Our results show that BOTFINDER is able to detect bots in network traffic without the need of deep packet inspection, while still achieving high detection rates with very few false positives.

BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection

Most of the current botnet detection approaches work only on specific botnet command and control (C&C) protocols (e.g., IRC) and structures (e.g., centralized), and can become ineffective as botnets change their C&C techniques. In this paper, we present a general detection framework that is independent of botnet C&C protocol and structure, and requires no *a priori* knowledge of botnets (such as captured bot binaries and hence the botnet signatures, and C&C server names/addresses). We start from the definition and essential properties of botnets. We define a botnet as a *coordinated group* of *malware* instances that are *controlled* via C&C communication channels. The essential properties of a botnet are that the bots communicate with some C&C servers/peers, perform malicious activities, and do so in a similar or correlated way. Accordingly, our detection framework clusters similar communication traffic and similar malicious traffic, and performs cross cluster correlation to identify the hosts that share both similar communication patterns *and* similar malicious activity patterns. These hosts are thus bots in the monitored network. We have implemented our BotMiner prototype system and evaluated it using many real network traces. The results show that it can detect real-world botnets (IRC-based, HTTP-based, and P2P botnets including Nugache and Storm worm), and has a very low false positive rate.

BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation

We present a new kind of network perimeter monitoring strategy, which focuses on recognizing the infection and coordination dialog that occurs during a successful malware infection. BotHunter is an application designed to track the two-way communication flows between internal assets and external entities, developing an evidence trail of data exchanges that match a state-based infection sequence model. BotHunter consists of a correlation engine that is driven by three malware-focused network packet sensors, each charged with detecting specific stages of the malware infection process, including inbound scanning, exploit usage, egg downloading, outbound bot coordination dialog, and outbound attack propagation. The BotHunter correlator then ties together the dialog trail of inbound intrusion alarms with those outbound communication patterns that are highly indicative of successful local host infection. When a sequence of evidence is found to match BotHunter’s infection dialog model, a consolidated report is produced to capture all the relevant events and event sources that played a role during the infection process. We refer to this analytical strategy of matching the dialog flows between internal assets and the broader Internet as dialog-based correlation, and contrast this strategy to other intrusion detection and alert correlation methods.

Towards Fingerprinting Malicious Traffic

The primary intent of this paper is detect malicious traffic at the network level. To this end, we apply several machinelearning techniques to build classifiers that fingerprint maliciousness on IP traffic. As such, J48, Na¨ıve Bayesian, SVMand Boosting algorithms are used to classify malware communications that are generated from dynamic malware anal-ysis framework.

Early Warning and Intrusion Detection based on Combined AI Methods
http://www.tzi.de/~edelkamp/secart2/papers/Fides.pdf

Detecting Stealthy Malware Using Behavioral Features in Network Traffic

https://www.cs.unc.edu/~reiter/theses/yen.pdf

http://www.mecs-press.org/ijisa/ijisa-v5-n3/IJISA-V5-N3-9.pdf

Talks

SQRRL

http://blog.sqrrl.com/an-introduction-to-machine-learning-for-cybersecurity-and-threat-hunting

https://speakerdeck.com/davidjbianco/getting-started-with-machine-learning-for-incident-detection

http://info.sqrrl.com/download-ueba-ebook

https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Brad-Woodberg-Malware-Command-And-Control-Channels-A-Journey-Into-Darkness.pdf

Code

https://github.com/DavidJBianco/Clearcut

Industry

https://www.patternex.com

Best Known:

http://blog.ventureradar.com/2016/03/11/10-hot-startups-using-artificial-intelligence-in-cyber-security/

HP ArcSight ThreatDetector and IBM QRadar use Machine Learning to automate pattern discovery and to facilitate intelligent rule creation

www.**ibm**.com/software/products/en/**qradar**-siem

https://www.f-secure.com/en/web/business_global/rapid-detection-service

https://jask.io/

Domain Generation Algorithms

https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/antonakakis

https://espionageware.blogspot.com/2014/04/apt-attributions-and-dns-profiling.html

General Knowledge

General

https://techcrunch.com/2016/07/01/exploiting-machine-learning-in-cybersecurity/

http://www.darkreading.com/vulnerabilities---threats/machine-learning-is-cybersecuritys-latest-pipe-dream/a/d-id/1322878?_mc=RSS_DR_EDT

http://www.dailydot.com/via/artificial-intelligence-cybersecurity-experts/

http://insidebigdata.com/2015/12/11/machine-learning-is-cybersecuritys-answer-to-detecting-advanced-breaches/

http://www.csoonline.com/article/3015670/security/machine-learning-cybersecurity-dream-come-true-or-pipe-dream.html

https://www.wired.com/2016/04/mits-teaching-ai-help-analysts-stop-cyberattacks/

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

c2

https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Brad-Woodberg-Malware-Command-And-Control-Channels-A-Journey-Into-Darkness-UPDATED.pdf

https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

http://essay.utwente.nl/61232/1/MSc_M_Warmer.pdf

Malware AI

http://www.jmlr.org/papers/volume13/tahan12a/tahan12a.pdf

How to do shit

https://github.com/paralax/awesome-honeypots

Offense AI

http://www.defenseone.com/technology/2016/08/artificial-intelligence-just-changed-future-information-security/130587/

I’m really good friends with these guys!

Defense AI

Fingerprinting C2 Servers

https://github.com/0x27/TheItalianJob

https://github.com/0x27/EquationSmasher

https://github.com/curesec/tools

https://www.sans.org/reading-room/whitepapers/detection/security-analytics-fun-splunk-packet-capture-file-pcap-34580

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.673.7452&rep=rep1&type=pdf

http://stackoverflow.com/questions/14090121/how-to-derive-kdd99-features-from-darpa-pcap-file

http://machinelearningmastery.com/how-to-prepare-data-for-machine-learning/