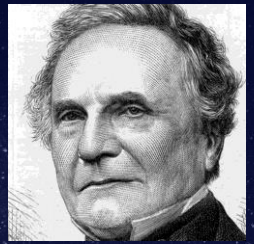
The Future of Cyber Intelligence

How Actionable Deep Learning is Changing the Face of Security

Derek Manky

FIT · FREEBUF

Early AI Defined

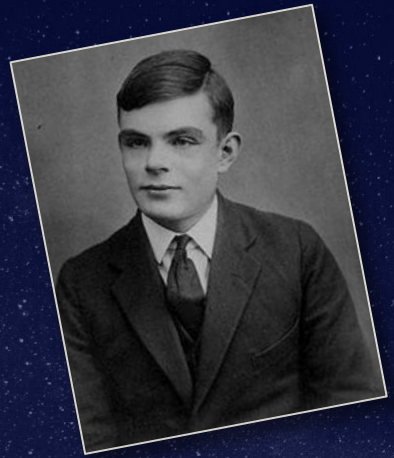


CHARLES BABBAGE
CREATED THE ANALYTICAL MACHINE IN 1837

ADA LOVELACE

- Worked with Babbage on engine
- Regarded as first computer programmer
- Created the first programmable algorithm
- Saw purposes for computing beyond just mathematical calculations

Early AI Defined



ALAN TURING
CALLED AN INFANT'S MIND AN 'UNORGANIZED MACHINE' IN 1930s

Created early definitions of machine learning

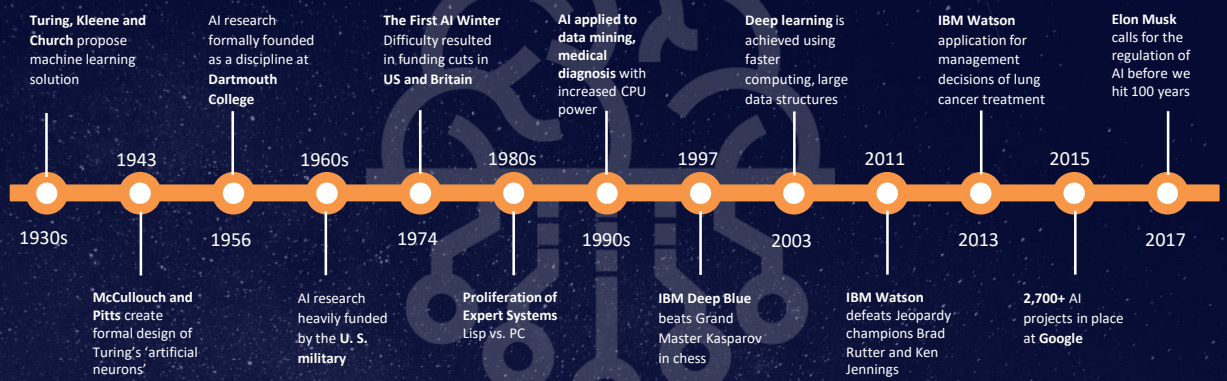
Saw the need for:

- Seeded solution set of accurate or known potential output
- Population of variably weighted pieces or functions
- A method for culling out the worst solutions while retaining the best

Major inhibitor of his research → was far ahead of available capabilities in terms of computing power

Artifical Intelligence - Nearing a Century

History of AI Outside Cyber Security Industry



1971: Creeper – The First Computer Virus

Creeper

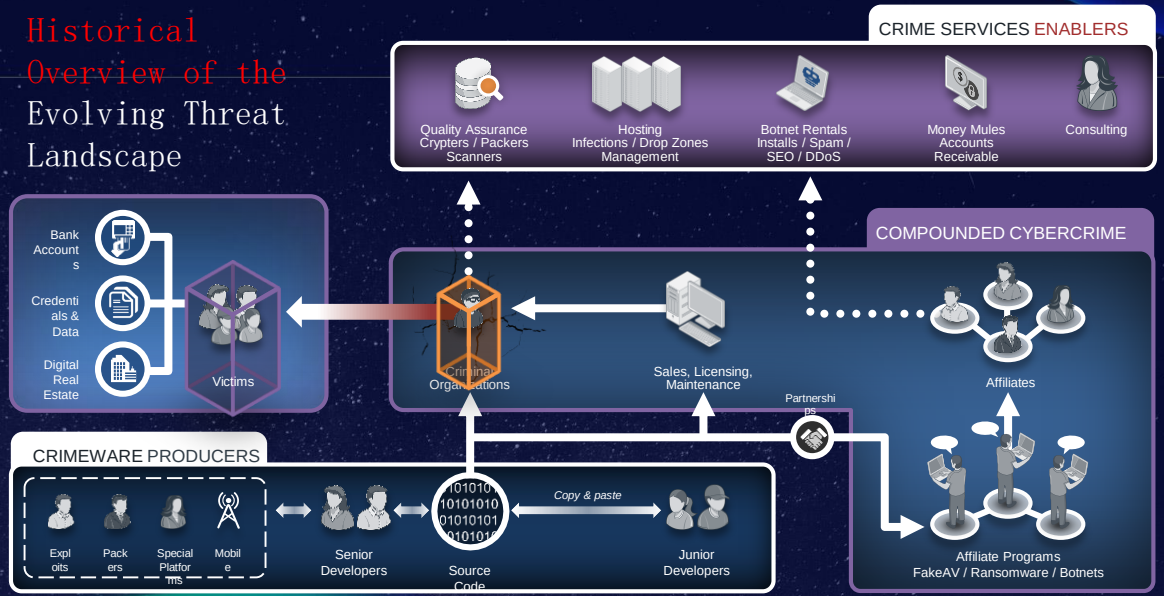
- Experimental self-replicating program
- Written in **1971** to demonstrate a 'mobile' application
- Infected DEC PDP-10 computers running TENEX OS
- Just 1 year after Unix 'Epoch Time' began
- 'Reaper' worm created in '72 to delete it

1 January 1970 00:00:00 GMT → Epoch timestamp 0

IM THE CREEPER, CATCH ME IF YOU CAN!

FortiGuard: One Minute in Cyberspace (Q3 2017)

Historical Overview of the Evolving Threat Landscape



FortiGuard Threat Intelligence Projects

CURRENT MEMBER COMPANIES

Expanding Globally: We publicly launched at RSA 2017 in February and now have *12 public Members.* We are actively engaged w/30+ global organizations to expand our footprint across the cyber ecosystem.

FOUNDING MEMBERS

Check Point SOFTWARE TECHNOLOGIES LTD.
CISCO
FORTINET
McAfee Together is power.
paloalto NETWORKS
Symantec

SOPHOS Security made simple.
Intsights
REVERSING LABS
RAPID7
SAINT
SK infosec
RSA
Eleven Paths Telefónica CYBER SECURITY UNIT

Board of Directors – Founding Members

Check Point SOFTWARE TECHNOLOGIES LTD.

Gil Shwed

CISCO

Martin Roesch

FORTINET

Ken Xie

intel Security

Chris Young

paloalto NETWORKS

Mark McLaughlin

Symantec

Greg Clark

WHY AN EXPERT SECURITY FABRIC IS NEEDED

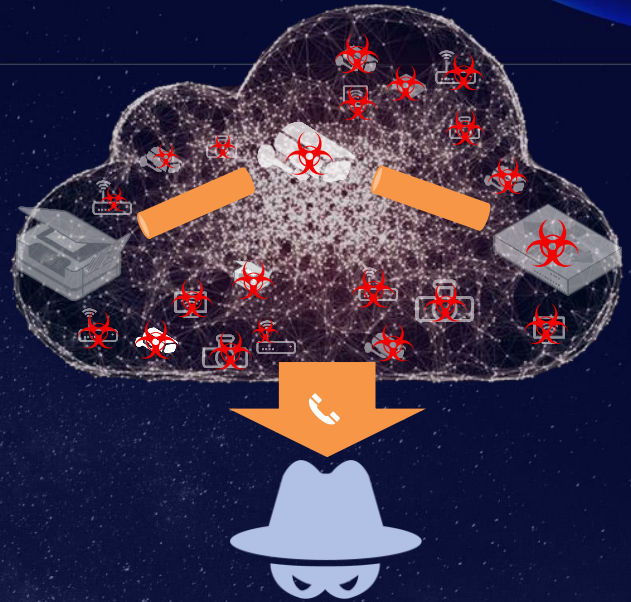
The Challenging Threat Landscape

AUTOMATED AND HUMAN-LIKE WILL DEMAND A MORE INTELLIGENT DEFENSE

Threats are getting smarter and are increasingly able to operate autonomously. In the coming year we expect to see malware designed "human-like" with adaptive, success-based learning to improve the impact and efficacy of attacks.

Threat Trends Hajime Botnet

- Intelligent IOT Botnet - Nine Platforms + x86
- TR-069 Exploit (MSSP/Telco Control)
- First detected October 25, 2016
- 30,000+ detections per day (FortiGuard)



PREDICTION:

THE RISE OF SELF-LEARNING HIVENETS AND SWARMBOTS

FIT · FREEBUF

PREDICTION:

RANSOM OF COMMERCIAL SERVICES IS BIG BUSINESS

FIT · FREEBUF

FIT · FREEBUF

PREDICTION:

NEXT-GEN MORPHIC MALWARE

FIT · FREEBUF

PREDICTION:

THE DARKWEB AND CYBERCRIME ECONOMY OFFER NEW SERVICES USING AUTOMATION

FIT · FREEBUF

FORTIGUARD EXPERT SOLUTIONS

Streamlining Intelligence with Service Providers

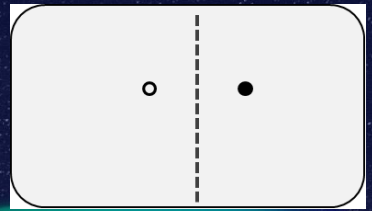
TECHNOLOGY WILL HAVE TO CLOSE THE GAP ON THE CRITICAL CYBER SKILLS SHORTAGE

Organizations simple do not have the experience or training necessary to develop a security policy, protect critical assets that now move freely between network environments, or identify and respond to today’ s more sophisticated attacks.

Machine Learning 101

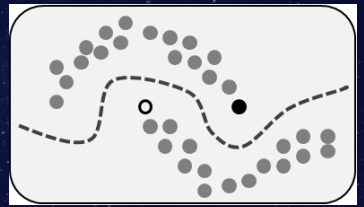
Supervised learning uses tags

- Eg: Input file is identified as malicious or clean
- AI initially feature set from initial files
- Weighted values are applied
- Expert humans may tone and guide feature sets



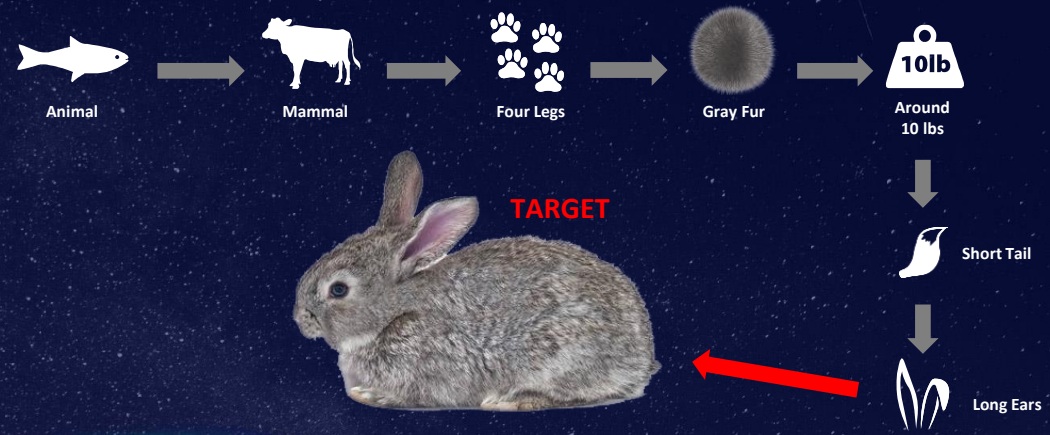
Unsupervised learning uses no tags

- Data is unlabeled; presents an unknown state to the AI
- Result is produced through inference
- Output is not evaluated for accuracy
- Unsupervised learning methods include
  - Clustering - creation of potentially new patterns
  - Anomaly detection - learn normal behavior and detect variances

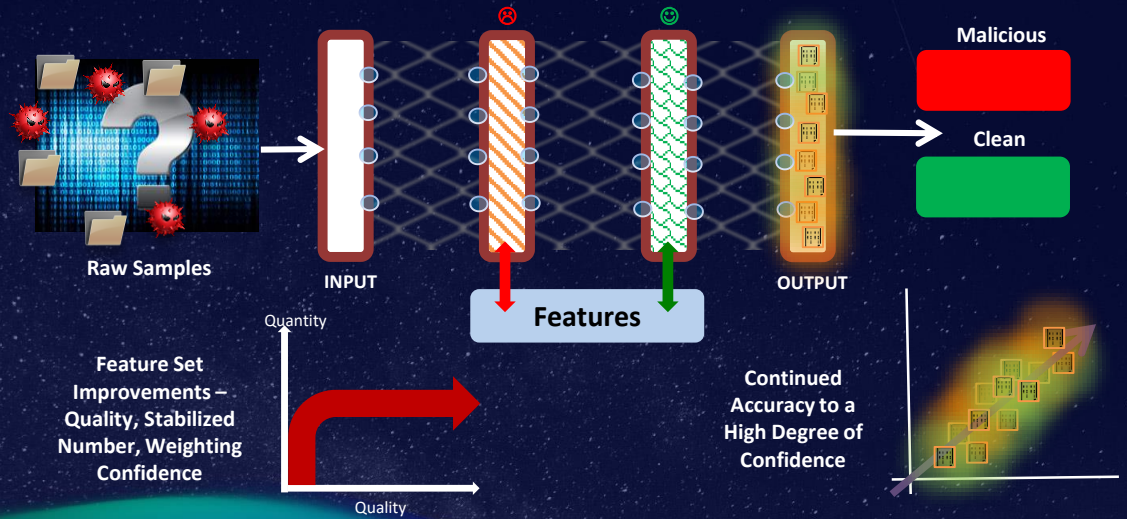


Machine Learning 101

Feature extraction - determine the object



FortiGuard Self Evolving Detection System



Fortinet Development Network

FNDN

Tiered Access

- Base (sponsored)
- Personal Toolkit
- Site Toolkit

Development Toolkit

- VM00 Licenses
- FortiClient Repackager
- FortiHypervisor (CE)
- FortiPlanner
- FortiCentral

FortiGuard Extensions

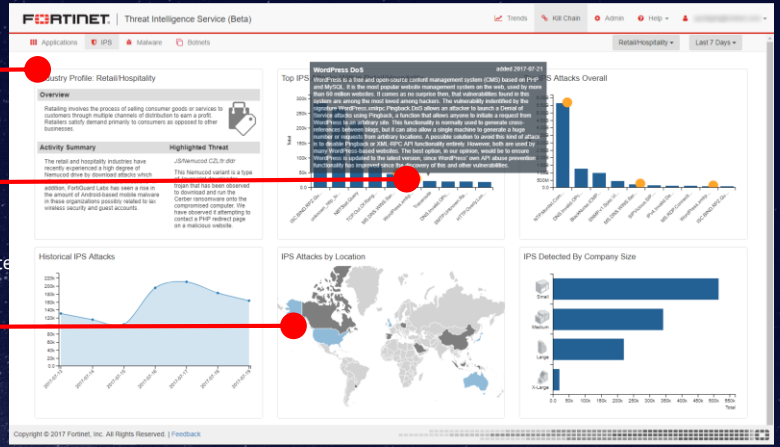
- Cyber Threat Intel (feed)
- FortiGuard.com Private Label
- Signature Lookup
- Web re-rating

FortiGuard TIS :: Kill Chain View

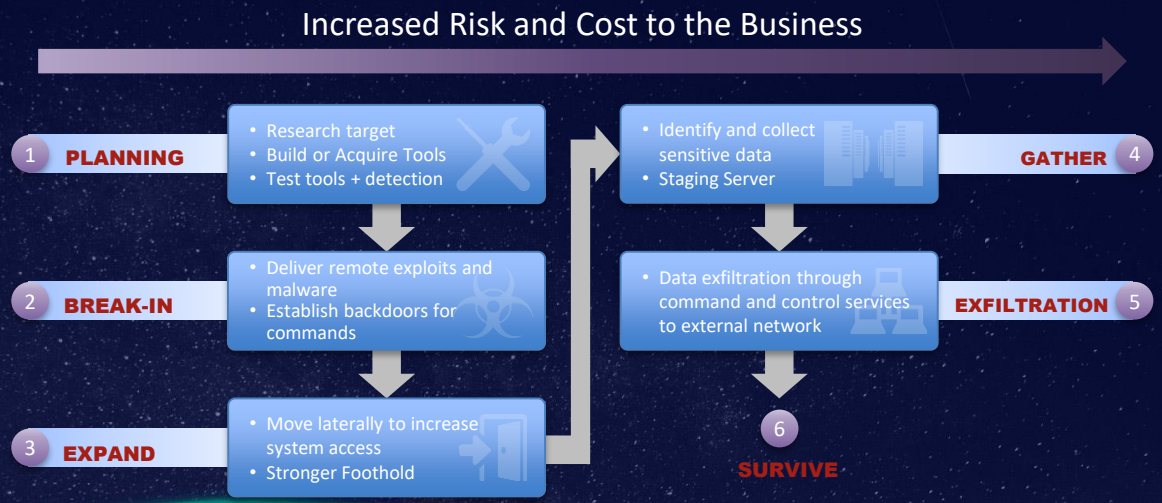
State of the Industry
Vertical profile information details specific industry threat levels

Campaign Commentary
FortiGuard Labs informs CISOs directly about why these risks matte
in near real-time

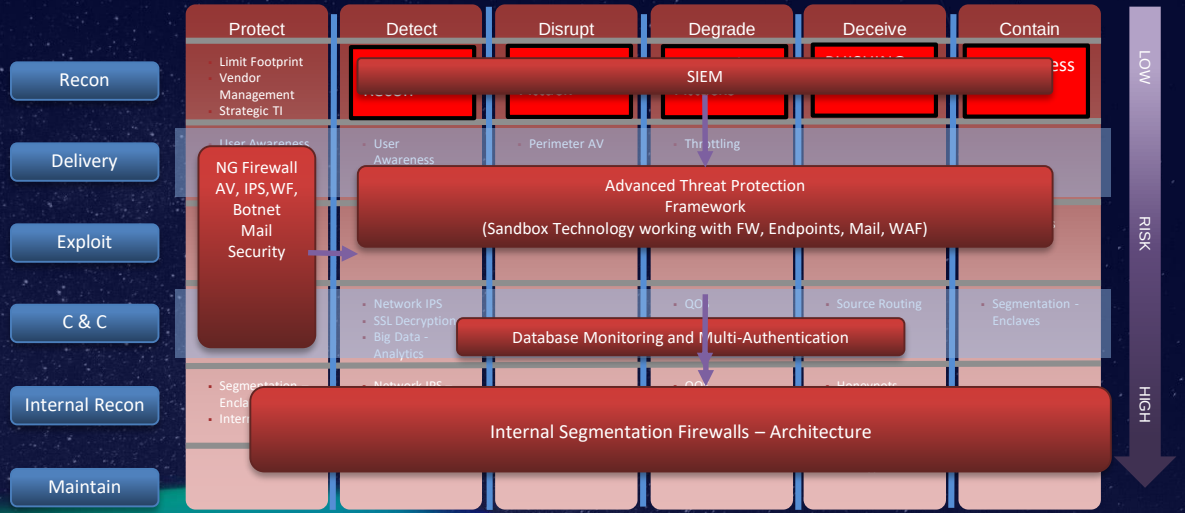
Threat Activity
A CISO can understand the threat landscape at large and how it will impact their organization



The Attack Chain



Threat Intelligence – Detailed Adversaries TTPs/Defenses



Definition

ex • pert sys • tem
noun
COMPUTING

a piece of software programmed using artificial intelligence techniques. Such systems use databases of expert knowledge to offer advice or make decisions in such areas as medical diagnosis and trading on the stock exchange.

Fortinet & FortiGuard: The Expert System

Crossing the "Last Mile": Creating Actionable Intelligence