Subverting AI:

Are we ready for a cyber pandemic ?

Who am I

- Co-Founder of PRODAFT
  (Proactive Defense Against Future Threats)

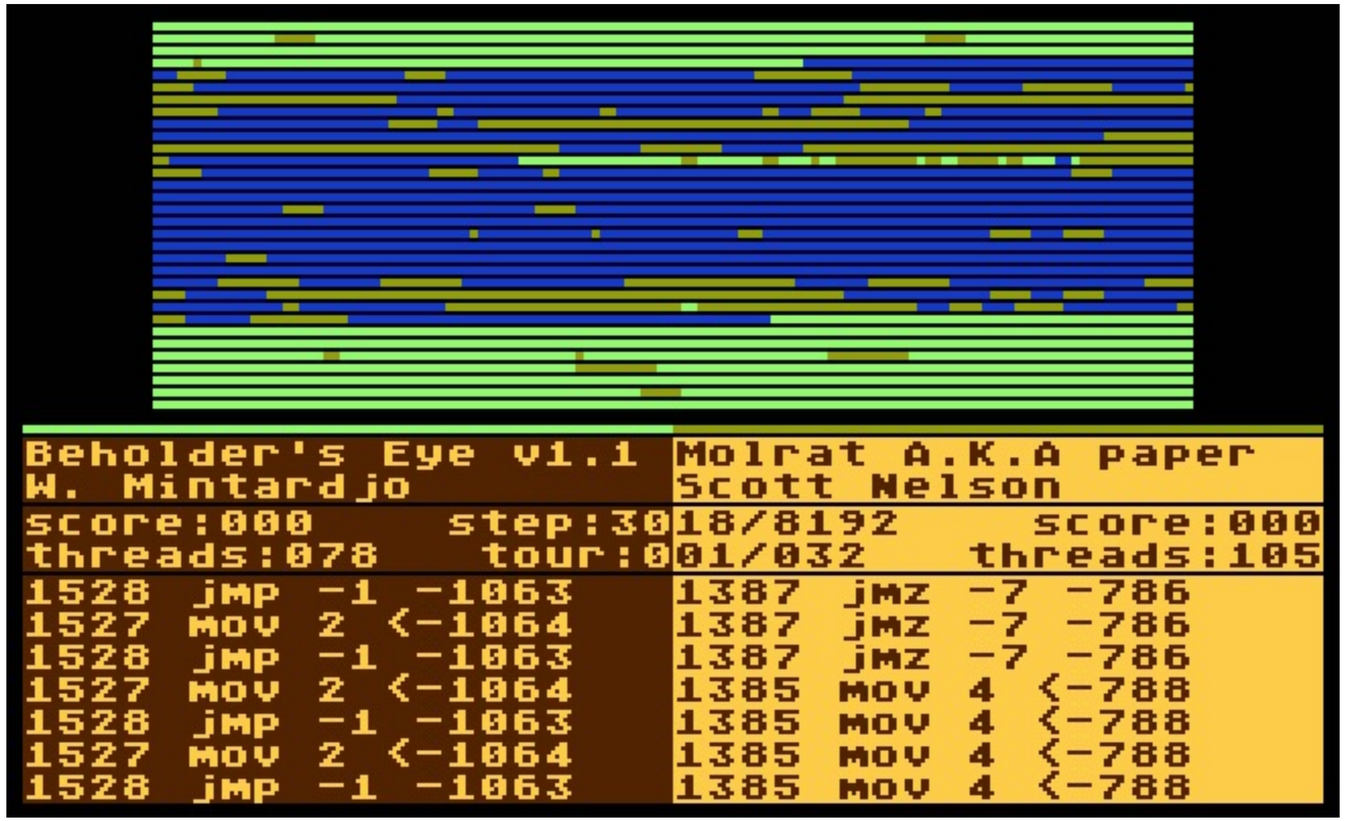
- +20 years of expertise in various fields such as cryptography, malware, covert channels, and digital forensics.

- Grand Champion – U.S. DoD DC3, 2011 Cybercrime Challenge.

- The Outstanding Young Persons – #1 Science & Technological Development JCI.

- Elected as one of the “Digital Shapers” of Switzerland

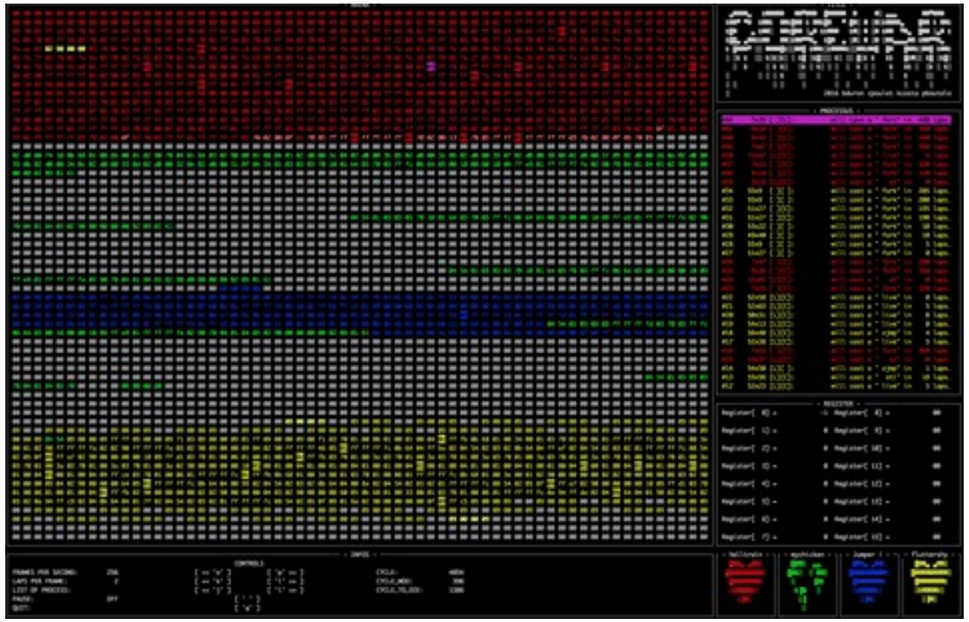
Historical Example: Defeating opponent’s code with AI

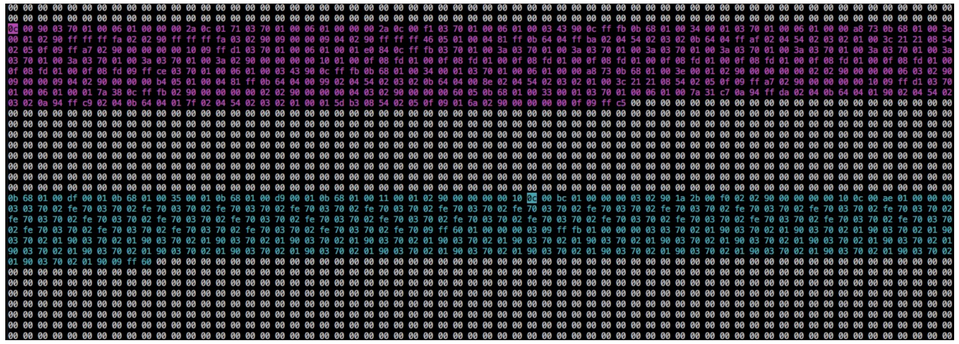


Historical Example: Core War

- 1984 programming game in which two or more battle programs (called "warriors") compete for control of a virtual computer.
- The objective is to kill your opponent's program by overwriting it.
- Primitive competition strategy.
- Inspired by Creeper, the first worm in history - 1971.
- Multiple ‘warriors’ developed over the years with limited learning capacity.

Historical Example: Core War

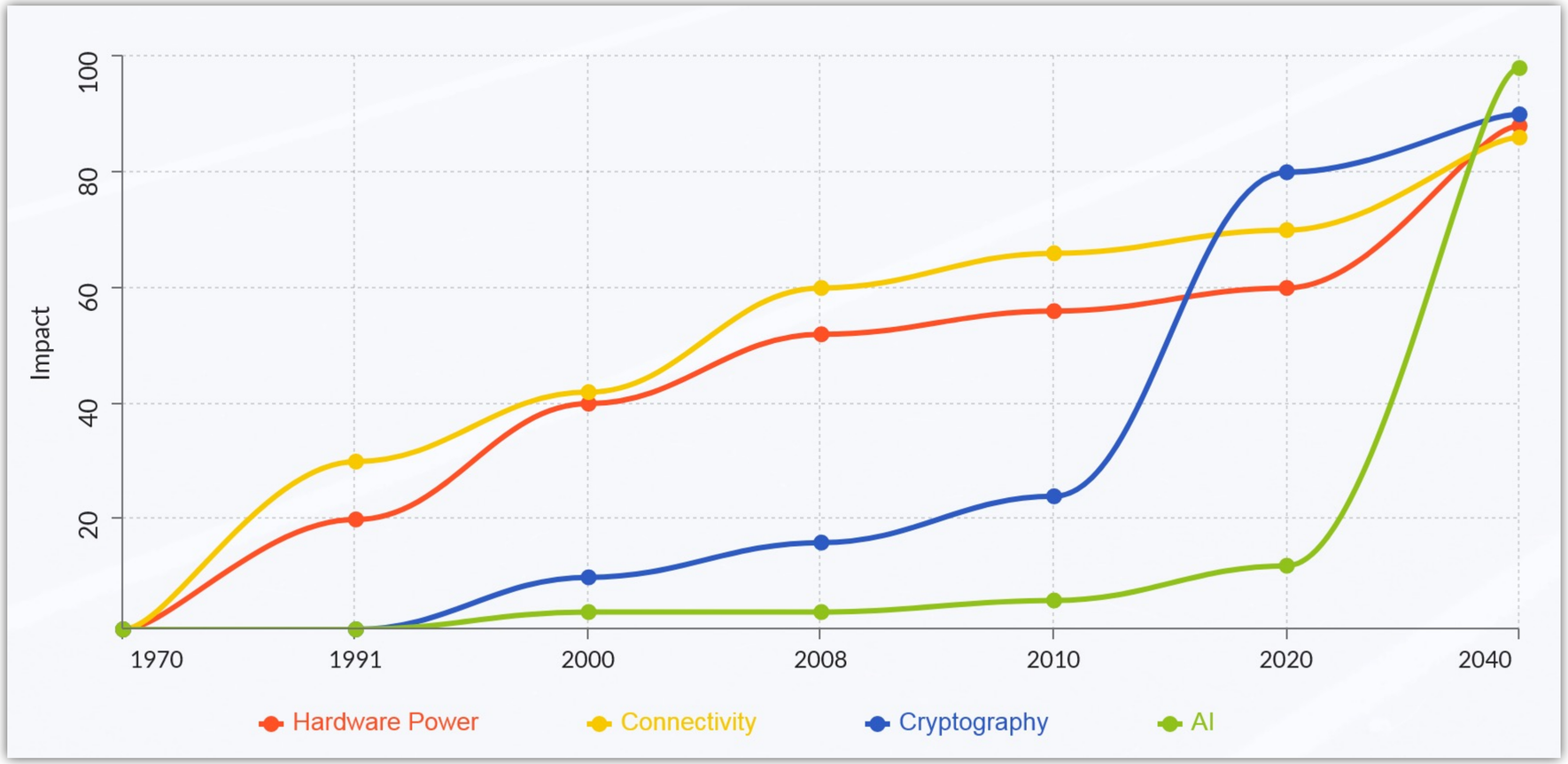




Core Wars Genetics: The Evolution of Predation
John Perry - UCLA Computer Science Department

Learning By Simulating Evolution Using Corewars
Ryan Coleman

Subverting different technologies



Malicious Cryptography - Cryptovirology

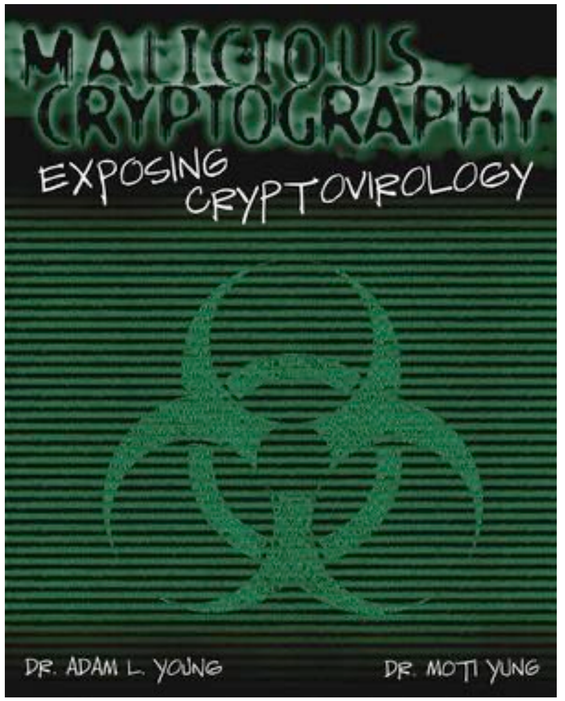
- Invented by Adam L. Young and Moti Yung

- “Cryptoviral extortion"

1996 IEEE Security & Privacy conference

“Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users. In this paper we present the idea of Cryptovirology which employs a twist on cryptography, showing that it can also be used offensively.”

Malicious Cryptography - 2004
- Non-Zero Sum Games and Survivable Malware
- Computationally Secure Information Stealing
- Cryptocounters



Comparison between malware and viruses

	Malware	Viruses
Spread	✚	✚
Self-Mutate	?	✚
Persistence	✚	✚
Survival	?	✚
Structure	Lines of code sequence	Lines of DNA sequence

- Can malware self-mutate ?
- How viruses evolve ?
- How can we introduce survival instinct ?

Viruses carry genetic material, reproduce, and evolve through natural selection.

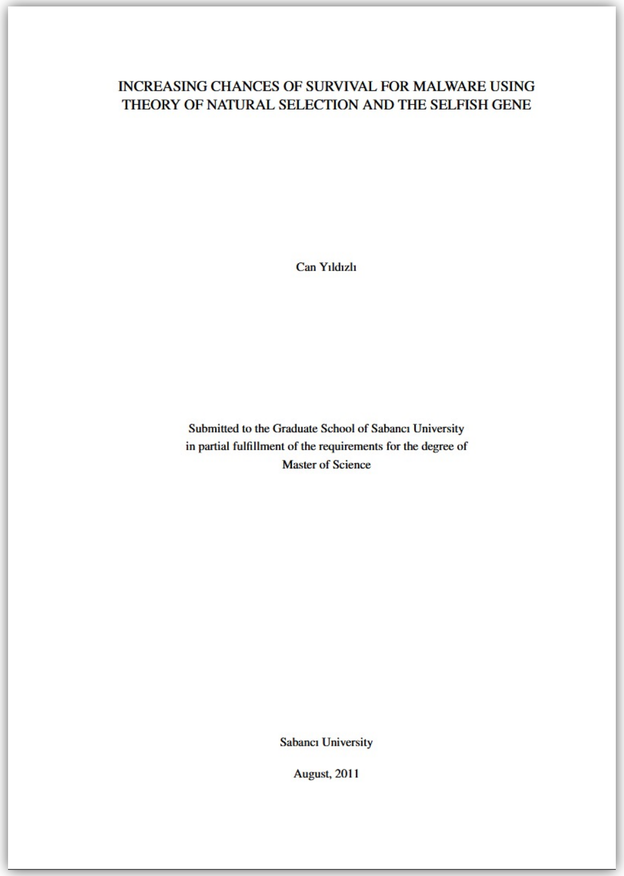
Viral populations do not grow through cell division, instead, they use the machinery and metabolism of a host cell to produce multiple copies of themselves, and they assemble in the cell.

How mutations happen ?

- Because mistakes do happen.
- Mutations can cause viruses to better evade our immune systems, treatments and vaccines.
- Mutations are not always good for the virus and most of them result in defective particles.

Subverting AI: Increasing chances of survival

- Propagation will not only change the representation of the code, but help to create new functionality
- Condition of “dying”
- Obtaining functionality from benign code
- Genetic algorithm to replicate itself
- Fitness function - Detection rate



INCREASING CHANCES OF SURVIVAL FOR MALWARE USING THEORY OF NATURAL SELECTION AND THE SELFISH GENE

Can Yıldızlı

Submitted to the Graduate School of Sabancı University
in partial fulfillment of the requirements for the degree of
Master of Science

Sabancı University

August, 2011

Emre Emin

- Senior Security Researcher @PRODAFT
- Computer Science & Mathematics
- Responsible for integration AI capabilities into cyber threat intelligence collection.
- Interests on the following subjects: cryptology, reverse engineering & exploitation, high performance computing and NLP.

Subverting AI: Environment Detection

- Execution environment is important as most of the suspicious executables are run in sandboxes, honeypots and virtual machines.
- Hardened environments are publicly shared and easy to re-create and populate.
- Each hardware and operating system have unique identifiers to be analyzed and most of the time it is better to do it least amount of tries. However, it is not only dependent to hardcoded and parametrized variables. There are also controls for relatively hard to measure and replay from known resources.

Subverting AI: Survival Instinct

- Sophisticated targeting and exploitation limits the attempts and opportunities.

- Execution lifetime is precious

- Running at the right time brings the strategic capability of

- Accessing more sensitive data
- Less noise
- Unpredictability

- Malware should be smart to adapt itself to the environment.

- Injection target
- Target behaviors (memory usage, allocation count, API calls etc.)

Subverting AI: Smart usage of ‘weapons’

- Malware often have spreading capability.
- Most of the time actions are noisy and requires an arsenal within the executable itself.
- It is important to use these weapons in an optimal way to decrease the noise created and get optimum outcome.

- Executing small number of SysCalls, sending a smaller number of requests and using less resources are better most of the time.

- Modern systems have more resources, but also have better monitoring.

- Detection systems are evolving
- Less is more

Subverting AI: Same host, same goal

- There are experiments on how malware work together on the same host.
- Although it may sound like more destructive, it is better to work together to increase their chance of survival by decreasing their effectiveness.
- Detection of one, means detection for everyone.
- We need to consider having variants of malware for every host.
- We can fasten this process easily. The question is: Are we ready for a cyber-pandemic ?

THANK YOU FOR LISTENING