# Ransomware vs AI. Part 2

## Bypassing Ransomware Protection with Reinforcement Learning

PRO.M.IS
security built in

**Professional Master in Information Security**

Alexander Adamov
oleksandr.adamov@bth.se

# In the previous episode


- AI & ML
- How AI can be used to detect ransomware
- Ransomware in 2019/20: LockerGoga and MegaCortex
- Ransomware bypassing techniques

# What’s new? WastedLocker

- 31 US-based organizations including Garmin have been successfully attacked
- Operated by the Evil Corp group
- Ransom request: $500,000 to over $10 million in Bitcoin
- Privilege escalation and defense evasion techniques:
  - Digital signing
  - Auto elevation (winsat.exe)
  - DLL side loading (winmm.dll)
  - Alternate Data Streams (ADS)
  - File memory mapping

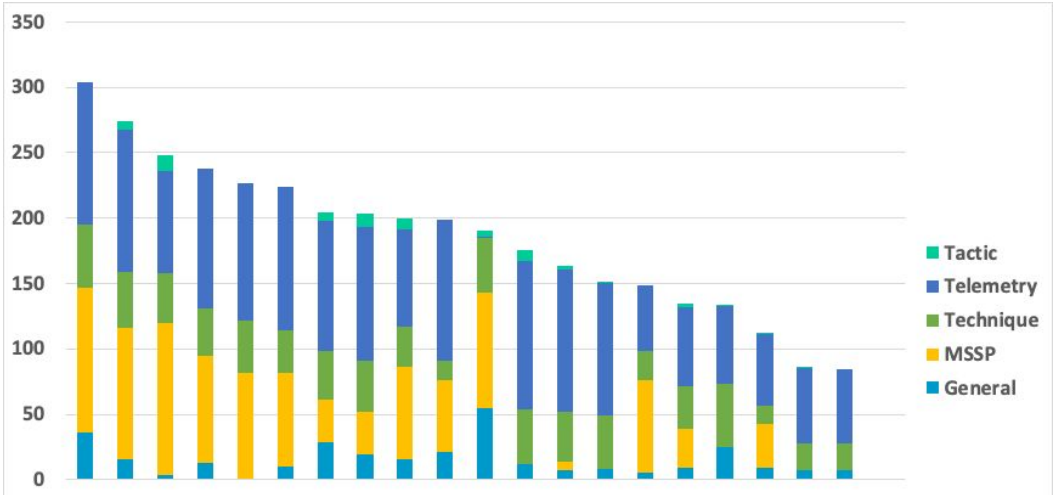
*“Generals are always prepared to fight the last war.”*

- Winston S. Churchill.

# Attack Simulation

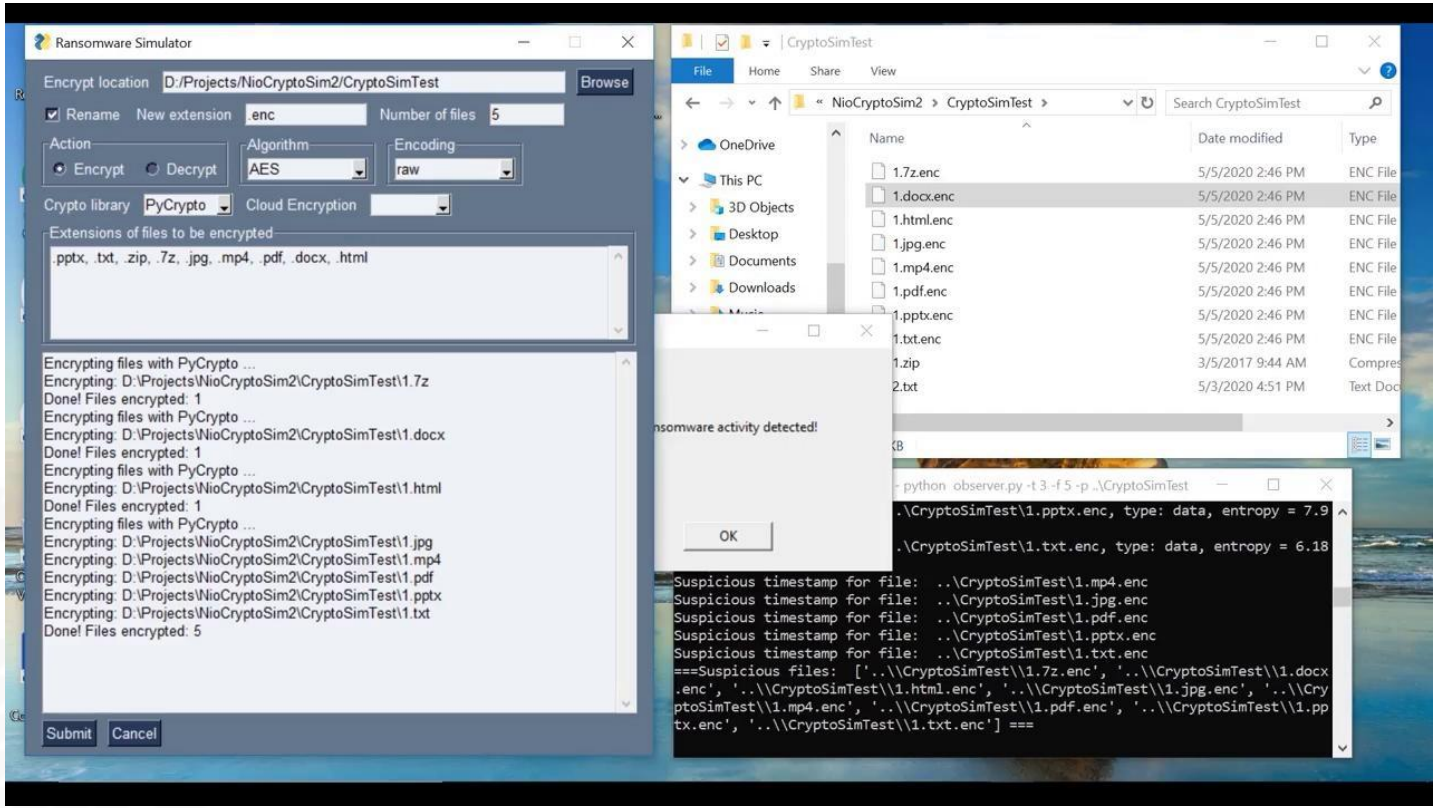
*It is possible to create a ransomware simulation that will use an arbitrary combination of* ***known tactics and techniques*** *to bypass an antivirus.*

APT29 attack simulation by MITRE ATT&CK
https://attackevals.mitre.org/

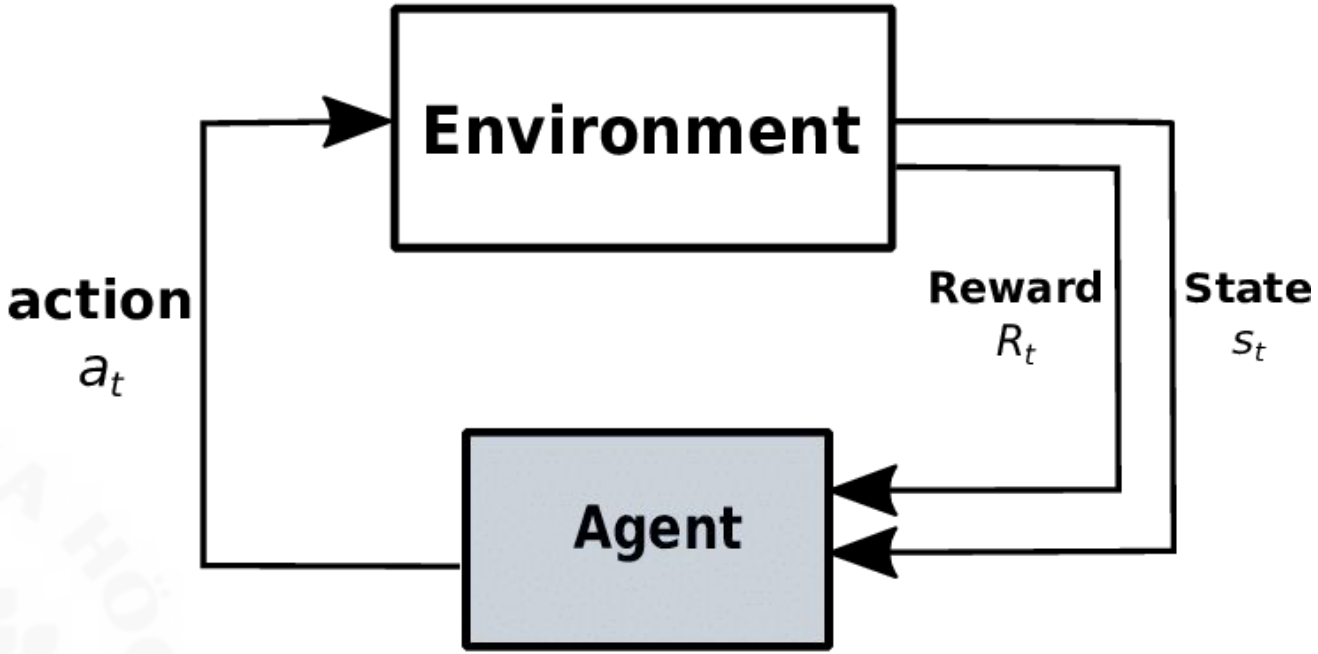



Source:
https://www.fireeye.com/blog/products-and-services/2020/04/mitre-evaluation-demonstrates-endpoint-security-managed-defense-detection-leadership.html

# Ransomware Simulation: Demo



# Reinforcement Learning



# Well-known RL algorithms

- AlphaGo defeated Lee Sedol - professional Go player of 9 dan rank and the 18-time world champion.
- 19x19 board
- $10^{360}$ possible moves


Source: https://deepmind.com/

# RL Actors

## 1) Ransomware Simulator

Goal: to encrypt the maximum number of files in the minimal number of steps

Options:

- Adding the specified extension (e.g. ‘.enc’)
- Encoding the AES encrypted data with Base64
- The number of files to be encrypted per step

## 2) Ransomware Detector

Goal: to detect files encryption and generate an alert

Detection methods:

- Checking for the the second extension
- Entropy level evaluation
- Anomalous files modification time detection

# States, Actions, Rewards

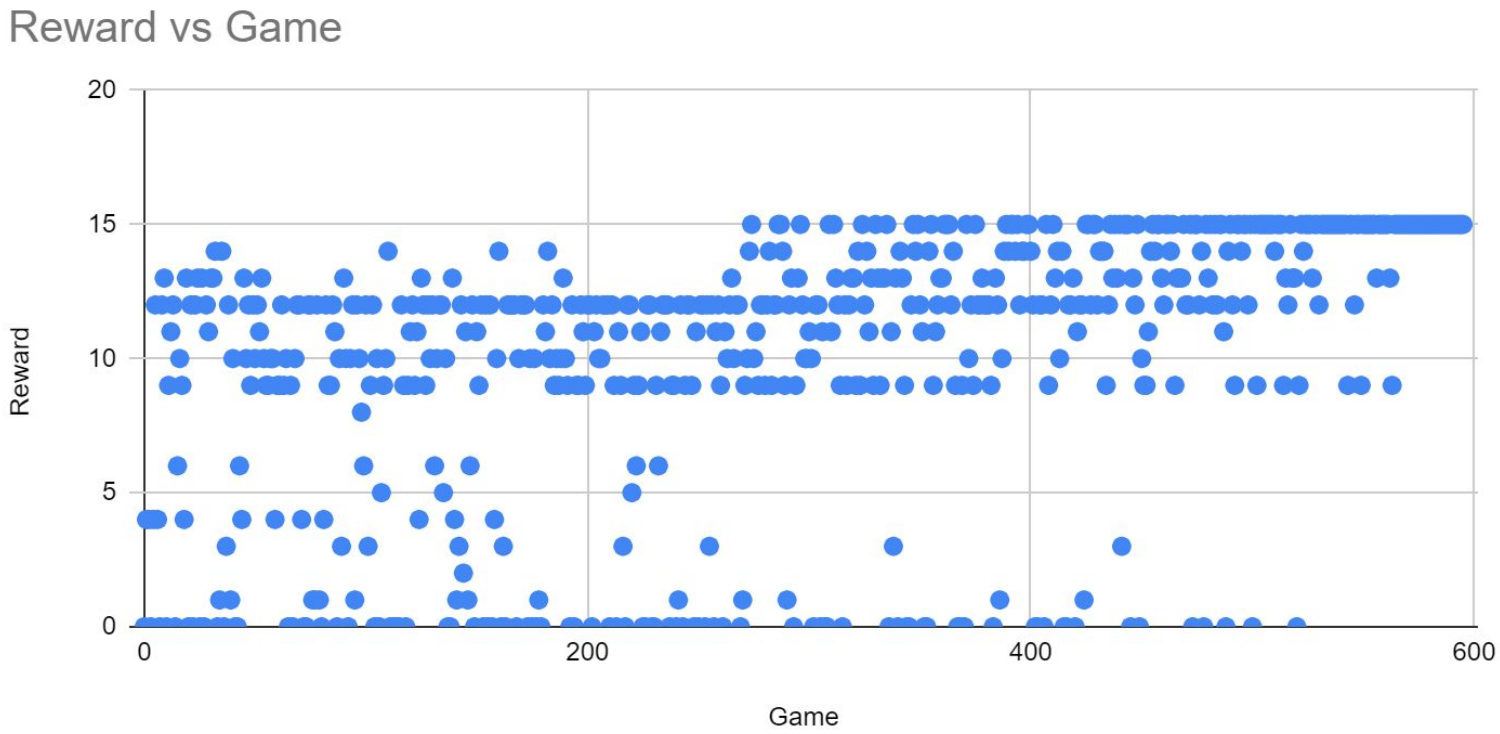
- States [0-10] - represents the number of encrypted files
- Rewards = encrypted_files * 2 - 1
  - 1 encrypted file = +2 points
  - 1 action = -1 point
- Actions (16)
  - Adding extension: {yes, no}
  - Base64 encoding: {yes, no}
  - The number of encrypted files per action: {1, 2, 5,10}

# Actions

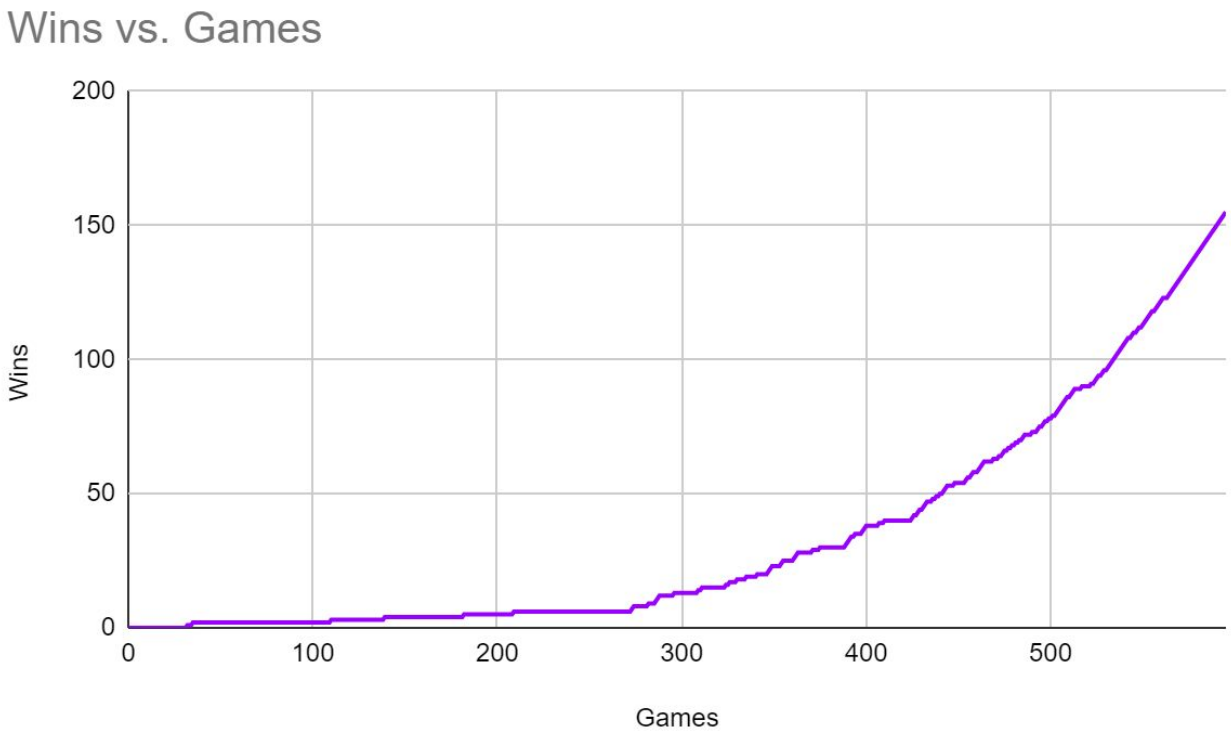
| Action type | Value 0 | Value 1 | Value 2 | Value 3 |
|---|---|---|---|---|
| Adding extension | no | yes | | |
| Base64 | no | yes | | |
| The number of encrypted files per execution | 1 | 2 | 5 | 10 |

| Action | Extension | Base64 | Number of Files |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 |
| 2 | 0 | 0 | 2 |
| 3 | 0 | 0 | 3 |
| 4 | 0 | 1 | 0 |
| 5 | 0 | 1 | 1 |
| 6 | 0 | 1 | 2 |
| 7 | 0 | 1 | 3 |
| 8 | 1 | 0 | 0 |
| 9 | 1 | 0 | 1 |
| 10 | 1 | 0 | 2 |
| 11 | 1 | 0 | 3 |
| 12 | 1 | 1 | 0 |
| 13 | 1 | 1 | 1 |
| 14 | 1 | 1 | 2 |
| 15 | 1 | 1 | 3 |

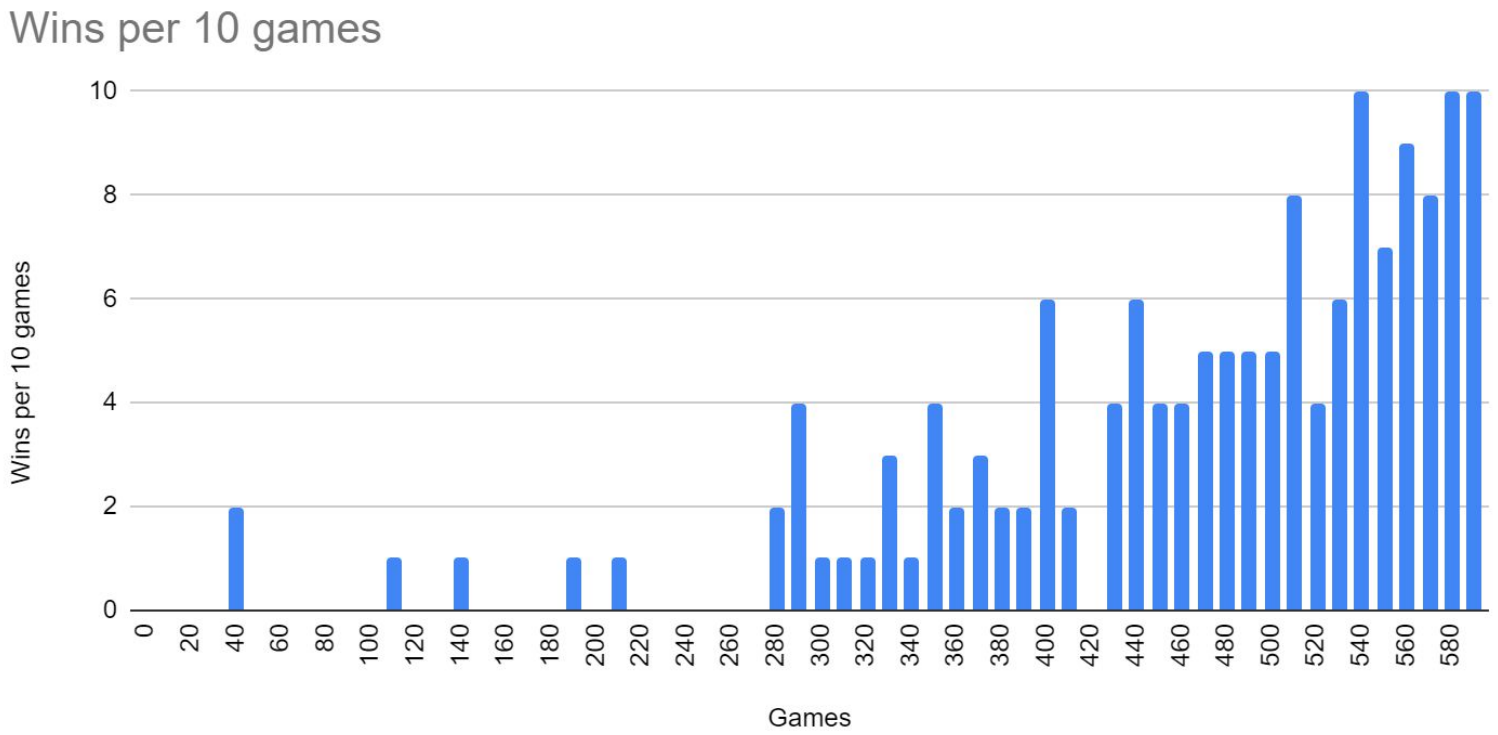
# Learning progress: Total Reward



# Wins vs. Games



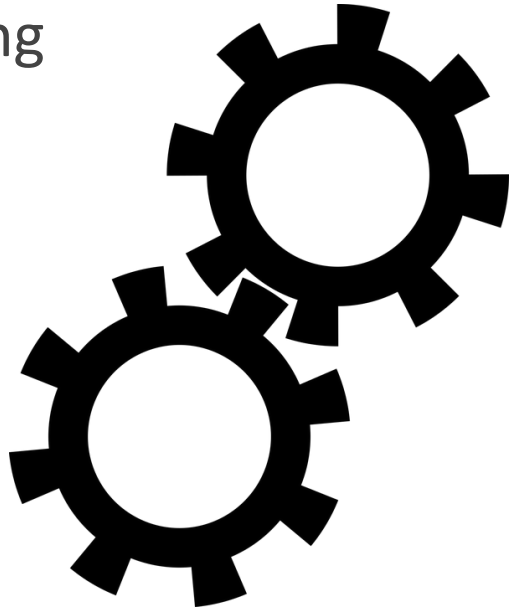
# Wins rate


Wins per 10 games
Wins per 10 games
10
8
6
4
2
0
0
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
320
340
360
380
400
420
440
460
480
500
520
540
560
580
Games

| Q (S, A) | States | | | | | | | | Threshold | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Actions | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 0 | 3.742632 | 0.787156 | 0.50037 | 0 | 0 | 1.007811 | 0.119928 | 2.686471 | 1.771443 | 0 | all files are encrypted |
| 1 | 7.105196 | 1.013578 | 1.252902 | 0.625865 | 0 | 5.491767 | 0 | 0.110781 | 0.020577 | 0 | |
| 2 | 7.545032 | 3.370516 | 1.118979 | 0.296561 | 0 | 1.170941 | 0.170201 | 0.147976 | 0.215866 | 0.763711 | |
| 3 | 6.681859 | 1.036887 | 1.431128 | 0 | 0 | 1.178761 | 0.10031 | 0.526232 | 0.019609 | 0.1805 | |
| 4 | 3.948145 | 0 | 0 | 0.231532 | 0.120758 | 0.790898 | 0.599471 | 0.871498 | 0.483216 | 0 | |
| 5 | 5.816442 | 0 | 1.158697 | 0.693802 | 0 | 1.778738 | 0.715084 | 0.205816 | 0.029846 | 0 | |
| 6 | 3.734055 | 8.923577 | 2.616297 | 0 | 0 | 0.747448 | 0.252802 | 0.236518 | 0.020577 | 0 | |
| 7 | 7.022468 | 0.056858 | 1.931174 | 0.563466 | 0 | 1.003211 | 0.213173 | 0.198259 | 0.377146 | 0 | |
| 8 | 4.158711 | 0.963861 | 1.045184 | 0 | 0 | 0.459586 | 0.590549 | 0.028423 | 0.28698 | 0.01805 | |
| 9 | 5.872631 | 0.463353 | 0.387103 | 0 | 1.524341 | 1.143632 | 0.358465 | 0.771859 | 0.112953 | 0.119148 | |
| 10 | 5.959267 | 0.9285 | 8.530923 | 1.739734 | 0 | 1.55761 | 0.141551 | 0.244138 | 0.172354 | 0 | |
| 11 | 6.141237 | 0 | 0.768712 | 0 | 0.144812 | 1.640483 | 0.149433 | 0.418004 | 0.055891 | 0.068169 | |
| 12 | 5.179697 | 1.992647 | 0.713766 | 0 | 0.443053 | 0.652553 | 0.226234 | 0.173608 | 0.372956 | 0.089291 | |
| 13 | 3.181544 | 1.945088 | 0.629294 | 0 | 0.422005 | 1.051774 | 2.283579 | 0.231025 | 0.166056 | 0 | |
| 14 | 14.11996 | 2.516235 | 1.889826 | 3.106087 | 0.087103 | 0.705648 | 0.275448 | 0.247926 | 0.20654 | 0 | |
| 15 | 5.828471 | 0.885469 | 0 | 0.163353 | 0 | 1.260362 | 0.080788 | 0.186429 | 0.010403 | 0.07444 | |

# Research in progress

1. Test on real anti-ransomware solutions
2. Apply in network and web penetration testing



# PROMIS (Professional Master in Information Security)

**GENERAL FORMAT**

**Active industrials studying and working at the same time**

- *University grade **COURSES for professionals**!*
- *Extend current competence in **an area ("security")***
- Case-based pedagogy (bring your own problems!)
- Online collaborative didactics
- Distance capability overall incl. lab and tools

**Courses under development with input from companies**

- Keep relevant and right level (companies advise us)
- DO YOU want to be part of the companies advising on courses?
  - CONTACT: Anna Eriksson aes@bth.se


SERL Sweden
LEADING SOFTWARE ENGINEERING

# Courses (3 thus far)

**PROMIS** (Professional Master in Information Security)

https://promisedu.se/


**Security in Software-intensive products and service development (**PA2582)
https://www.bth.se/eng/courses/D5818/20202/
Course responsible: Tony Gorschek
tony.gorschek@bth.se

- The ability to understand the technology, operational aspects, and
  engineering aspects of security - albeit the focus on the course is on "engineering security"
- The ability to plan for "pre-emptive" security in the planning and development of products and services
- The ability to do a risk assessment and take ROI into account
- The ability to develop and use secure architectures that allows for a more stable base for products and services
- The ability to compare and weigh the benefits and costs of non-functional aspects in combination to security
- The ability to estimate how security aspects impact, and are impacted on quality-/non-functional aspects such as usability, performance and maintainability of a product

*more to come*

# Courses (3 thus far)

**PROMIS** (Professional Master in Information Security)

https://promisedu.se/

**Software Security (**DV2595)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: Dragos Ilie dragos.ilie@bth.se

- The ability to  understand how attackers exploit risky programming practices
- The ability to detect risky programming practices
- The ability to understand and reason about efficiency and limitations in existing software security mechanisms
- The ability to to compare and weight the benefits and costs associated with binary analysis and instrumentation techniques


*more to come*

SERL Sweden
LEADING SOFTWARE ENGINEERING

# Courses (3 thus far)

**PROMIS** (Professional Master in Information Security)
https://promisedu.se/


**Web System Security (**DV2596)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: Anders Carlsson
anders.carlsson@bth.se

- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to describe the Common Vulnerability Scoring System (CVSS)
- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to explain the security aspects when using languages and framework, eg. PHP, JavaScript, and SQL
- be able to explain authentication mechanisms and counter techniques to bypass authentication
- understand Cross-site scripting (XSS) attacks and SQL injections
- be able to explain impacts of one or more combined vulnerabilities that limit or extend the damage given
- be able to install and configure the web server for high security independently
- be able to use and search open vulnerability databases (Common Vulnerability databases CV -DB)

to prevent and find security problems

- be able to use best practice of known design patterns for secure web applications
- be able to utilize OWASP where applicable
- be able to conduct internal and external penetration testing of web applications and related infrastructure)

*more to come*

# PROMIS

**Spread information about courses @ your company**

## HOW TO APPLY

https://promisedu.se/

**Entry Requirements**

*PROMIS courses requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).*

Even if you don't have the formal academic merits, you might be qualified for the course through validation (reell kompetens)!

**Apply for course:**

1. **Create a user account at antagning.se / universityadmission.se**
2. **Search for PROMIS courses by the name Fill in and send in your application**
3. **Upload your required documents (employer's certificate)**
4. **Reply to any offers of admission**

**Questions about the course:** contact course responsible
**Questions about applying and validation (reell kompetens): :** anna.eriksson@bth.se
Visit promisedu.se for more info about courses, application and template for employer's certificate