Tom Gonda

Year of Birth: 1988, Address: Weizman 35, Hertzelia, Israel
Email: tom.gonda@gmail.com, Phone: 0546511988

About me

I'm a hands-on security researcher and team leader with experience in windows internals (WinDbg, IDAPro). Additional experience includes network protections (Check Point) and academic research (Attack Graphs). I'm interested in a hands-on low level research role.

Education

2016-2017: M.Sc. Software and Information Systems (fast-track, cyber-security sub-field), BGU - 89 avg

2012-2016: B.Sc. Software Engineering (graduation with honors), BGU - 88 avg

2011: Psychometric score – 750

Work Experience

2017-Present: Nyotron Information Security (Endpoint protection)

2019-Present: Security Research Team Leader

- Leading research, design and implementation of security, FP reduction and usability features
- Devising and prioritizing the product's security roadmap

2018-2019: Managed Defense Services Team Leader

- Responsible for customer's security and business continuity
- Recruiting and training 5 analysts. Some of them later detected real-world sophisticated attacks
- Improved the team's performance by automating many day-to-day tasks saving hundreds of analyst hours

2017-2018: Senior Security Researcher

- Investigating attacks on customer's networks and producing reports
- Improving the product's protection logic. Some of the improvements prevented PTs and live attacks

2016-2018: Freelance consultant at Intelici (Graph based prediction startup)

- Developer at a machine-learning graph-based fake news detection POC (Twitter)
- Development, deployment and maintenance of a network flow-based attack detection POC (ISP level)

2016-2017: Researcher and Developer at Deutche Telecom Labs

- Research focused on attack graphs – graphical model which represents an adversary attacking enterprise organizations. The research includes producing datasets using vulnerability scanners and developing algorithms using Pyhon's Networkx library
- In addition, developer at a project for dynamic collection of forensic evidence in enterprise networks. Contributed to the development, architecture and testing. Programming in Java, DB - MSSQL

2014-2015: Security Analyst at Check Point

- Writing IPS (IDS) signatures for the IPS engine and conducting research to support it
- Developer in a team building a framework for dynamic execution of malwares (Cuckoo)

Army Service

2009-2011: Intelligence Officer – Research Department (Aman)

2007-2009: Analyst – Research Department (Aman)

Tools & Frameworks

Research, Reversing & Debugging:

- IDA Pro (+IDAPython)
- Windbg (+preview) including kernel debugging
- Sysinternal suite & extensions (procmon, api-mon, etc)

Programming:

- Python (Mainly Pycharm)
- C/C++ (Visual studio)
- Java (IntelliJ)

Machine Learning:

- Keras (tensorflow backend)
- Genism
- Scikit-learn
- nltk

Graphs:

- Networkx (python)
- Gephi

Projects & Publications

- Analysis of reddit's AITA subreddit (NLP) - https://medium.com/@tom.gonda/what-does-reddit-argue-about-28432b11ea26 *2019*
- OilRig Incident Report – Nyotron (https://nyotron.com/oilrig). *2018*
- PyEye – Eye tracking using simple webcam - https://github.com/tomgond/pyEye *2018*
- Gonda, Tom, el al. "Analysis of Attack Graph Representations for Ranking Vulnerability Fixes" *GCAI, 2018*
- Gonda, Tom, et al. "Ranking vulnerability fixes using planning graph analysis." *IWAISe: First International Workshop on Artificial Intelligence in Security*. *2017*.
- Gonda, Tom, el al. "Scalable attack path finding for increased security" *International Conference on Cyber Security Cryptography and Machine Learning. 2017*