Igor Korkin, Ph.D

E-mail: igor.korkin@gmail.com
Phone: +7 (903) 523-77-12
Skype: igor2igor
Homepage: http://bit.ly/igorkorkin

Summary

A fan of digital security, full of passion and curiosity, I have an ambition to improve the anti-malware protection systems utilizing machine learning techniques and to hunt zero-day exploits. Cyber security determinates my life: it is my job, but also my hobby and lifestyle. My areas of expertise are kernel mode rootkit detection, Windows internals and hardware virtualization technologies (Intel VT-x, EPT, PT). I have published more than 20 research papers; 5 recent papers are double-blind peer reviewed.

Education

2009-2012 **Moscow Engineering Physics Institute**. Department of Cryptology and Discrete Mathematics.
Degree: Ph.D. in Computer Science.
Thesis topic: "Statistical Detection of Hardware Virtualization Based Rootkits".

2004-2009 **Moscow Engineering Physics Institute**. Department of Cryptology and Discrete Mathematics.
Degree: MSc in Computer Science, diploma with distinction.
Master topic: "Stealth Malware Detection System in OS Windows".

Work History

Senior Researcher, Russian Research Institute, Moscow, Russia February 2009 – present

- Kernel-mode driver development and user-mode applications using C/C++, WDK, VS, WinDbg;
- Cyber security and digital forensics research in various expert teams;
- Various docs and publications for customers.

Awards

- 1st place in the «Hackers vs. Forensics» challenge, «Positive Hack Days Forum», Moscow, Russia (2012).
- 3rd place at «Microsoft Summer School on the Internet of Things» (IoT security team project), Kazan, Russia (2016).
- Highly appreciated peer-reviewed publication at the Conference on Digital Forensics, Security and Law, Daytona Beach, Florida, USA (2015).

My Recent Research Projects:

2017 *Detect Kernel-Mode Rootkits via Real Time Logging & Controlling Memory Access*,
Korkin, I., Tanda, S., 12th Annual Conference on Digital Forensics, Security and Law, USA
http://igorkorkin.blogspot.com/2017/03/memorymonrwx-detect-kernel-mode.html

2016 *Monitoring & Controlling Kernel-Mode Events by HyperPlatform*,
Korkin, I., Tanda, S., REcon conference, Canada
http://igorkorkin.blogspot.ru/2016/06/monitoring-controlling-kernel-mode.html

2016 *Acceleration of Statistical Detection of Zero-day Malware in the Memory Dump Using CUDA-enabled GPU Hardware*,
Korkin, I., Nesterow I., 11th Annual Conference on Digital Forensics, Security and Law, USA
http://igorkorkin.blogspot.ru/2016/05/acceleration-of-statistical-detection.html

2015 *Two Challenges of Stealthy Hypervisors Detection: Time-Cheating and Data Fluctuations*,
Korkin, I., 10th Annual Conference on Digital Forensics, Security and Law, USA
http://igorkorkin.blogspot.ru/2015/05/two-challenges-of-stealthy-hypervisors.html

2014 *Applying Memory Forensics to Rootkit Detection*,
Korkin, I., Nesterow I., 9th Annual Conference on Digital Forensics, Security and Law, USA
http://igorkorkin.blogspot.ru/2014/07/applying-memory-forensics-to-rootkit.html