Igor Korkin, Ph.D. in CS Windows Security Researcher

igor.korkin@gmail.com github.com/igorkorkin igorkorkin.blogspot.com

Summary

I am a fan of cross-disciplinary security research in the field of Windows OS kernel. My areas of expertise include detection and prevention of rootkits, memory forensics, and hardware virtualization technologies. My research results were presented at **Black Hat Europe 2018**, **REcon 2016**, six **ADFSL conferences 2014-2019**, and **RusCrypto 2011**.

Education

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

Moscow Engineering Physics Institute. Department of Cryptology and Discrete Mathematics. 2004-2009
Degree: *Master of Science in Computer Science, Cyber Security*.
Master topic: “Stealth Malware Detection System in OS Windows”.

Work History

Lead Security Research Engineer,
Special System Engineering Centre (ssec.ru), Moscow, Russia March 2019 – now

- Development of the advanced firewall system for Windows-based hosts using C/C++, STL, and Npcap.
- Presenting current results at conferences.

Senior Researcher,
FGUP CNIIHM (www.cniihm.ru), Moscow, Russia February 2009 – March 2019

- Development of kernel-mode drivers and user-mode applications using C/C++, VS, WDK, WinDbg;
- Cyber security and digital forensics research in different expert teams;
- Various docs, publications, and presentation for customers.

Main Awards

- 1st place in the «Hackers vs. Forensics» challenge at PHDays Conference, Moscow, Russia (2012);
- 3rd place at «Microsoft Summer School on the Internet of Things», Kazan, Russia (2016);
- One of the best papers award at the 10th ADFSL Conference, Daytona Beach, Florida, USA (2015).

Recent Research Projects

2019 ***MemoryRanger Prevents Hijacking FILE_OBJECT Structures in Windows Kernel***
Korkin, I., 14th ADFSL Conference, Daytona Beach, Florida, USA
https://igorkorkin.blogspot.com/2019/04/memoryranger-prevents-hijacking.html

2018 ***Divide et Impera: MemoryRanger Runs Drivers in Isolated Kernel Spaces***,
Korkin, I., Briefings at Black Hat Europe, London, UK
http://bit.ly/MemoryRanger

2018 ***Hypervisor-Based Active Data Protection for Integrity and Confidentiality of Dynamically Allocated Memory in Windows Kernel***,
Korkin, I., 13th ADFSL Conference, San Antonio, Texas, USA
http://bit.ly/AllMemPro

2017 ***Detect Kernel-Mode Rootkits via Real Time Logging & Controlling Memory Access***,
Korkin, I., Tanda, S., 12th ADFSL Conference, Daytona Beach, Florida, USA
http://bit.ly/MemoryMonRWX

2016 ***Monitoring & Controlling Kernel-Mode Events by HyperPlatform***,
Korkin, I., Tanda, S., REcon Conference, Montreal, 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 ADFSL Conference, Daytona Beach, Florida, 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 ADFSL Conference, Daytona Beach, Florida, 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 ADFSL Conference, Richmond, Virginia, USA
http://igorkorkin.blogspot.ru/2014/07/applying-memory-forensics-to-rootkit.html