Igor Korkin, Ph.D.

Lead Security Researcher & Developer
Digital Security Expert
Team Lead

igor.korkin@gmail.com
github.com/igorkorkin
sites.google.com/site/igorkorkin

SUMMARY

Solid cybersecurity expert with 15+ years of experience in OS security research, specializing in Windows and Linux systems across user, kernel, and hypervisor levels. Expert in rootkit detection, memory forensics, attacks on AV/EDR, sandboxing and bare-metal hypervisors. Consistently combines theoretical knowledge and practical expertise to drive cutting-edge research innovations, transforming them into market-leading products that outperform competitors. Currently developing breakthrough security systems to detect advanced threats in both Linux and Windows environments. Published **40+ research papers** and **one patent**. My research results were presented at **15+ conferences**: HITB 2023 (Thailand), EKOPARTY 2022 (Argentina), ROOTCON 2022 (Philippines), LABScon 2022 (USA), **BlackHat 2022 (USA)**, **BlackHat 2021 (UK)**, Texas Cyber Summit 2021 (USA), **IEEE SP SADFE 2021 (USA)**, HITB 2020 (Singapore), **BlackHat 2018 (UK)**, REcon 2016 (Canada), seven ADFSL conferences 2014-2022 (USA), RusCrypto 2011 (Russia).

EDUCATION

Moscow Engineering Physics Institute (eng.mephi.ru), Moscow, Russia
Department of Cryptology and Cybersecurity (kaf42.mephi.ru)

- **Ph.D., Cybersecurity and Computer Science** — 2009.09-2012.08
  Dissertation: Detection Hidden Virtualization-Based Malware
- **M.S., Cybersecurity and Computer Science** — 2004.09-2009.08
  Thesis: Detection Hidden Malware in Windows Kernel

PROFESSIONAL EXPERIENCE

Lead Software Developer — 2023.10 – Present
Positive Technologies (1 year), Moscow, Russia

Summary:

- Dedicated to enhancing business security solutions in anticipation of evolving malware threats, I specialize in developing breakthrough strategies to combat advanced cyber threats.

Key Achievements regarding Multiscanner and PT Sandbox:

- Develop advanced plugins for business products: implementation fast and secure kernel-mode code.
- Design cutting-edge engines for Extended Detection and Response (XDR), Malware Analysis, and Advanced Threat Detection (Sandbox).
- Implement and enhance an integrated unit testing framework for Windows kernel drivers.
- Integrate code check rules into the CI/CD pipeline to ensure code quality and security.
- Solve code compatibility issues across various OS versions
- Experience with full software development life cycle, including coding standards, code reviews, source control management, build processes, testing, and operations
- Product Feature Owner: New Advanced Feature to struggle with APT malware.

Lead Security Researcher, Expert
LLC Ventra (3 years), Huawei Technologies (0,7 year), Russia, China 2019.11 –2023.08

Summary:

- Grade 19 (Expert B) | Probationary Period: Excellent (2023-02) | Two business trips to China | Defended Competency and Qualification (C&Q) Level 4 in 2023-08.
- Focused on proactively improving Huawei's business solutions in data security, privacy, and system trustworthiness to make the products resilient against advanced cyberattack techniques.
- Research and Develop of Proof of Concept (POC) and Minimum Viable Product (MVP)

Details:

- Contributed pivotal technological breakthroughs that were integrated into business products WUCS (memory protection and anti-code injections in Windows OS), EulerOS (SBM, memory protection, see patent), Dorado (integrated security system to protect files from human-based threats: ransomware, file corruption).
- Research Protection Mechanisms of Linux and their robustness against rootkits using OS-level technologies (achievement: published a patent and SandBox Mode is integrated into the kernel) and hypervisor-based technologies (Applying MemoryRanger principle to isolate LKM from the kernel). Details of OS-level protection:
  → Google Patents - US20230289465A1- https://patents.google.com/patent/US20230289465A1/en
  → WIPO Patent Scope - WO2022105610 - https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2022105610
  → Huawei SandBox Mode (SBM) prevents vulnerability exploitation via decomposing the kernel - https://lwn.net/Articles/962087/
- Research Algorithms to protect Windows Huawei Applications from common user-level intrusions (achievement: team award)
- Research Data Storage Protection Technologies (prepared and defended Strategic Planning; completed H1 stage in 2023-07)
- Presented at various Huawei events.
- Received personal and team awards.

Huawei Honors & Awards:

- Huawei Future Star Award 2022
  → Research and Develop new Data Storage Protection Technologies to detect Ransomware Attacks and File Corruption Attacks (Data Wiping).
  → Chong-Ming Lab Managers: Ma Chun Fei (马春飞), Hu Gang and Huang Mengyu
- Windows Security Team - Excellent Team Award 2021 - Cloud Service Competence Center
  → Research and Develop user-level components for Windows Unified Crypto Service (WUCS)
  → Research and Develop Algorithms to protect Windows OS Huawei Applications from common user-level attacks
  → VIKA lab Managers: Liu PinPing (刘玭娉katelyn) and Evgeny Smirnov

Details of Huawei Patent:

- Inventors: Hu Kekai (an expert from HQ, Shenzhen, China) and Igor Korkin (Moscow, Russia)
- Title: Data protection method and device, storage medium and computer equipment
- CN114519186A - https://patents.google.com/patent/CN114519186A/en
- US20230289465A1 - https://patents.google.com/patent/US20230289465A1/en
- EP4231181A1 - https://patents.google.com/patent/EP4231181A1/en

Position: Lead Security Research Engineer
Special System Engineering Centre (ssec.ru), Moscow, Russia 2019.03 –2019.10

- Developed Windows-based firewall system using C/C++, STL, and Npcap;
- Presented research results at conferences.

Position: Senior Researcher
FGUP CNIIHM (www.cniihm.ru), Moscow, Russia 2009.02 – 2019.03

- Developed kernel-mode drivers and user-mode applications using C/C++, VS, WDK, WinDbg
- Conducted cybersecurity and digital forensics research in various expert teams
- Produced documentation, publications, and presentations for customers.

Publishing Systems Records:

- arXiv - https://arxiv.org/a/korkin_i_1.html
- ORCID - https://orcid.org/0000-0001-7640-2792
- DBLP - http://dblp.uni-trier.de/pers/hd/k/Korkin:Igor
- IEEE - https://ieeexplore.ieee.org/author/37088908930
- OpenReview - https://openreview.net/profile?id=~Igor_Korkin1
- Semantic Scholar - https://www.semanticscholar.org/author/3114387
- SCOPUS - https://www.scopus.com/authid/detail.uri?authorId=57219459633
- Google Scholar Citations - https://scholar.google.com/citations?user=0RJh3vYAAAAJ

PROFESSIONAL ACTIVITIES

Program Committee Member

- State Examination Board, Moscow Engineering Physics Institute, Moscow, Russia

Journal Reviewer

- Journal in Computer Virology, Springer Nature, France, Online
- Journal of Computer Virology and Hacking Techniques, Springer Nature, France, Online

ADVISING

Visiting Professor (volunteering)
Moscow Engineering Physics Institute (eng.mephi.ru), Moscow, Russia 2013.09 – Present

Summary:

- Supervising research works for post-graduate and Ph.D students
- Experience as a mentor, tech lead of various security research projects
- More than 30 graduates have obtained diplomas; they are employed in top Russian and Chinese companies.

Students diploma titles:

- Stealthy malware detection system in Windows x64 (2014-2016)
- Nested virtualization detection system (2014-2016)
- Applying Event Trace for Windows (ETW) to detect malware behavior (2015-2017)
- Memory Forensics of Windows x64 (2015-2017)
- Spyware detection framework for Android (2015-2017)

- Detection of encrypted file containers with deliberately decreased entropy (2016-2018)
- Applying ETW and machine learning to detect illegal cryptocurrency mining (2017-2019)
- Detection of rootkits with deliberately spread code sections in Windows memory (2017-2019)
- RASP for LSASS: Preventing Mimikatz-Related Attacks (2021-2023)
- ALPChecker – Detecting Spoofing and Blinding Attacks (2021-2023)
- Human-Controlled Fuzzing With AFL (2021-2023)
- Security analysis of Windows Defender AV (2022-2024)
- Attacks on Microsoft Defender via Process Sandboxing (2021-2023)

Open-Source Contribution

- [C\C++, SDK, WDK, Windows 7-11] **Research and Develop MemoryRanger Project**
  MemoryRanger protects kernel data and code by running drivers and hosting data in isolated kernel enclaves using VT-x and EPT features. MemoryRanger has been presented at worldwide conferences including BlackHat, HITB, CDFSL https://github.com/IgorKorkin/MemoryRanger
- [C, SDK, Windows OS] **Vulnerability research and analysis for open-source software**:
  - LZ4 (issues: #926, #927, #929), fix: https://github.com/lz4/lz4/blob/48d9b7416b4c4ef89ac8ad3fc6b2fff7bcb8a870/NEWS
  - OpenVPN (several new DoS attacks on OpenVPN protocol were implemented)

International Cooperation:

- **Satoshi Tanda, Canada, 2016-2017**
  - Task: develop a new generation of hypervisor for Windows, research, develop PoC
  - Results: [9] and [10]
- **Binarly, USA, LA, 2020-2022**
  - Task: analyze architecture weakness of modern AV/EDR, research, develop PoC
  - Results: [2] and [3]
- **Huawei, China, 2019-2023**

Languages

- Russian (Native)
- English (Professional working proficiency)

Publishing Systems Records – The recent research projects:

1. ALPChecker – Detecting Spoofing and Blinding Attacks
   Hack In The Box Security Conference (#HITB2023HKT #COMMSEC), Oct 25, 2023, Thailand

2. Blasting Event-Driven Cornucopia: WMI-based User-Space Attacks Blind SIEMs and EDRs
   BlackHat USA, Las Vegas, USA, August 6-11, 2022.

3. Veni, No Vidi, No Vici: Attacks on ETW Blind EDR Sensors
   BlackHat Europe Conference, London, UK, November 10-11, 2021.

4. Protected Process Light will be Protected – MemoryRanger Fills The Gap Again
   Systematic Approaches to Digital Forensic Engineering (SADFE) International Workshop;

2021 IEEE Symposium on Security and Privacy Workshops, San Francisco, USA, May 24-27, 2021.
Texas Cyber Summit IV, Oct 29–30, 2021, USA, TX, San Antonio.

5. Windows Kernel Hijacking is Not an Option: MemoryRanger Comes to the Rescue Again
   Hack In The Box Security Conference (HITBLockdown002), July 25, 2020, Singapore
   Journal of Digital Forensics, Security and Law, USA, June 10, 2021.

6. MemoryRanger Prevents Hijacking FILE_OBJECT Structures in Windows Kernel
   ADFSL Conference, Daytona Beach, Florida, USA, May 15-16, 2019.

7. Divide et Impera: MemoryRanger Runs Drivers in Isolated Kernel Spaces
   BlackHat Europe Conference, London, UK, December 5-6, 2018.

8. Hypervisor-Based Active Data Protection for Integrity and Confidentiality of Dynamically Allocated Memory in Windows Kernel
   ADFSL Conference, Daytona Beach, Florida, USA, May 17-18, 2018.

9. Detect Kernel-Mode Rootkits via Real-Time Logging & Controlling Memory Access
   ADFSL Conference, Daytona Beach, Florida, USA, May 17-18, 2017.

10. Monitoring & controlling kernel-mode events by HyperPlatform
    REcon conference, Montreal, Canada, 17-19 June 2016.

11. Acceleration of Statistical Detection of Zero-day Malware in the Memory Dump Using CUDA-enabled GPU Hardware
    ADFSL Conference, Daytona Beach, Florida, USA, May 24-25, 2016.

12. Two Challenges of Stealthy Hypervisors Detection: Time Cheating and Data Fluctuations
    ADFSL Conference, Daytona Beach, Florida, USA, May 19-21, 2015.

13. Applying Memory Forensics to Rootkit Detection
    ADFSL Conference, Daytona Beach, Florida, USA, May 28-29, 2014.