Black Hat USA 2018

Toshihito Kikuchi

Keynote: Optimistic Dissatisfaction with the Status Quo: Steps We Must Take to Improve Security in Complex Landscapes

- Abstract
- Parisa Tabriz | Director of Engineering, Google
- Black Hat USA 2018 Keynote: Parisa Tabriz - YouTube https://www.youtube.com/watch?v=py2qmGbyhlw
- Google's effort to change the industry
  - Project Zero
    - improve vendor's priority, grab public attention, and broad attack knowledge
  - HTTPS journey
    - *"Making fundametal change to the status quo is hard but necessary. If you're not upsetting anyone, you're not changing the status quo."*
  - Chrome's Site Isolation
    - started in 2012 with 10 persons
    - *"No one have predicted something as big as Spectre, but we all need to continue investing in ambitious proactive defensive projects like site isolation."*
    - *"A lot of the most impactful security work in large projects is not adding new things and adding more complexity but simplifying existing code or systems since that inevitably leads to better security."*

New Trends in Browser Exploitation: Attacking Client-Side JIT Compilers

- Abstract
- Samuel Groß | Independent Researcher
- https://saelo.github.io/presentations/blackhat_us_18_attacking_client_side_jit_compilers.pdf
- V8's new engine
  - Ignition interpreter
  - Turbofan compiler

Subverting Sysmon: Application of a Formalized Security Product Evasion Methodology

- Abstract
- Lee Christensen | Senior Red Team Operator/Hunt Analyst, SpecterOps
Matt Graeber | Security Researcher, SpecterOps
- https://github.com/mattifestation/BHUSA2018_Sysmon

Why so Spurious? How a Highly Error-Prone x86/x64 CPU "Feature" can be Abused to Achieve Local Privilege Escalation on Many Operating Systems

- Abstract
- Nemanja Mulasmajic | Anti-Cheat Engineer,
  Nicolas Peterson | Anti-Cheat Engineer
- http://i.blackhat.com/us-18/Wed-August-8/us-18-Mulasmajic-Peterson-Why-So-Spurious.pdf
- MOV/POP SS vulnerability (CVE-2018-8897)
  http://everdox.net/popss.pdf

The Problems and Promise of WebAssembly

- Abstract
- Natalie Silvanovich | Security Engineer, Google
- http://i.blackhat.com/us-18/Thu-August-9/us-18-Silvanovich-The-Problems-and-Promise-of-WebAssembly.pdf

The Windows Notification Facility: Peeling the Onion of the Most Undocumented Kernel Attack Surface Yet

- Abstract
- Alex Ionescu|Kernel Ninja, Winsider Seminars & Solutions, Inc.
  Gabrielle Viala|Security Engineer, Quarkslab
- WNF example: Feature Control Multi-tool
  https://github.com/riverar/mach2
- Any user-mode process can subscribe lots of interesting events (WiFi connection, Edge browsing, Power state, etc.)
- My write-up and code
  - https://qiita.com/msmania/items/aaba5f3bddec10c245c8
  - https://gist.github.com/msmania/472912cd6e9ab067be3211ba3f5f0f9e

Decompiler Internals: Microcode

- Abstract
- Ilfak Guilfanov | CEO, Hex-Rays SA
- http://i.blackhat.com/us-18/Thu-August-9/us-18-Guilfanov-Decompiler-Internals-Microcode.pdf
- Hex-Rays Decompiler generates its own IR to decompile

Wrangling with the Ghost: An Inside Story of Mitigating Speculative Execution Side Channel Vulnerabilities

- Abstract
- Anders Fogh | Principal Security Research, G DATA Advanced Analytics
Christopher Ertl | Security Engineer, Microsoft
(Matt Miller | Partner Security Software Engineer, Microsoft)
- https://github.com/Microsoft/MSRC-Security-Research/blob/master/presentations/2018_08_BlackHatUSA/us-18-Fogh-Ertl-Wrangling-with-the-Ghost-An-Inside-Story-of-Mitigating-Speculative-Execution-Side-Channel-Vulnerabilities.pdf

Windows Offender: Reverse Engineering Windows Defender's Antivirus Emulator

- Abstract
- Alexei Bulazel | Security Researcher, ForAllSecure
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Bulazel-Windows-Offender-Reverse-Engineering-Windows-Defenders-Antivirus-Emulator.pdf
- Some static analysis tools
  - CPU emulator based on QEMU https://github.com/unicorn-engine/unicorn
  - Code coverage https://github.com/gaasedelen/lighthouse
- Windows Defender on Linux
  - https://github.com/taviso/loadlibrary
  - https://github.com/0xAlexei/WindowsDefenderTools

Hardening Hyper-V through Offensive Security Research

- Abstract
- Jordan Rabet | Senior Security Software Engineer, Microsoft
- http://i.blackhat.com/us-18/Thu-August-9/us-18-Rabet-Hardening-Hyper-V-Through-Offensive-Security-Research.pdf

Meltdown: Basics, Details, Consequences

- Abstract
- Daniel Gruss|Postdoctoral Researcher, Graz University of Technology
  Michael Schwarz|University Assistant, Graz University of Technology
  Moritz Lipp|University Assistant, Graz University of Technology
- Technically, nothing new from their paper
  https://arxiv.org/abs/1801.01207
- Often-heard misunderstandings:
  - Is Meltdown a speculative execution? -- NO
  - Is Meltdown a side-channel attack? -- NO