



OFF-BY-ONE 2025

DAY 1 MAY 8TH

8:45am - 9:25am	Registration
9:25am - 9:35am	Welcome Address
9:35am - 10:20am	Keynote: Spyware for rent & the world of offensive cyber - Fred Raynal
10:20am - 11:05am	Patch Diffing, You Are My Sword! A Deep Dive into Two Critical N-day Vulnerabilities in FortiGate - Qian Chen & Zibo Li
11:05am - 11:25am	Coffee Break
11:25am - 12:10pm	Exploitation Against the Clock: Xiaomi S3 Smartwatch - Sergei Volokitin
12:10pm - 12:55pm	Bug Bounty: my cottage industry of crime - Jim Rush
12:55pm - 2:05pm	Lunch
2:05pm - 2:50pm	Speed up your reverse engineering with the hrtng plugin - Georgy Kucherin
2:50pm - 3:35pm	COM-pletely Unplanned: A Windows Bug Hunter's Journey to LPE - Dongjun Kim & Jongseong Kim
3:35pm - 4:05pm	Coffee Break
4:05pm - 4:50pm	When ASUS IoT Devices Play Hide-and-Seek with Security: A Vulnerability Adventure - swing, chumen77 & fcx233
4:50pm - 5:35pm	S.H.I.E.L.D: Scudo Heap Implementation Exploits, Leaks, and Defenses - Tom Mansion
5:35pm - 6:20pm	A Journey into Windows Security Support Provider Interface - Yuki Chen

DAY 2 MAY 9TH

9:00am - 09:20am Collect Day 2's Wristband

9:20am - 10:05am Keynote: If you don't care about a vulnerability, why should I? - **James Forshaw**

10:05am - 10:50am Security Cracks at the Summit: Rethinking OTA Updates
- **EunGyo Seo, Hea Eun Moon & Hyunseok Yun**

10:50am - 11:10am Coffee Break

11:10am - 11:55am JAAS is All You Need: Reviving JDBC Again and Again
- **Zhou Ji'an, Zhu Ying & Izy**

11:55am - 12:40pm The Matrix Unloaded: Escaping the JTAG Reality
- **Thomas Serpinis**

12:40pm - 1:50pm Lunch

1:50pm - 2:35pm Breaking Decompilers - **Jordan Wiens**

2:35pm - 3:20pm Simple is Best: The journey of taking over mobile system using a GPU logical bug - **Shang Hongze**

3:20pm - 3:50pm Coffee Break

3:50pm - 4:35pm Don't Believe The Hype(rvisor) - **Daniel Komaromy & Laszlo Szapula**

4:35pm - 5:20pm Five years of hacking ICS/IoT in Pwn2Own
- **Sharon Brizinov**

5:20pm - 5:30pm Closing Remarks



SPONSORS



eShard

Quarkslab



StealthMole



INTfinity

ISD