kaspersky

# SECURITY ANALYST SUMMIT

October 25–28, 2023
Phuket, Thailand

## October 25th

| | | |
|---|---|---|
| All day | Arrivals | |
| 15:00-00:00 | Hotel check in | **JW Marriott Phuket resort**<br>231 Moo 3 Mai Khao, Talang, Phuket, Thailand, 83110 |
| 14:00-22:00 | Registration for #TheSAS2023 | **Mai Khao Ballroom prefunction area**<br>JW Marriott Phuket resort |
| 19:30-22:00 | Welcome dinner | **Andaman Grill restaurant**<br>JW Marriott Phuket resort |

## October 26th

| | | |
|---|---|---|
| 07:00-09:30 | Breakfast | **JW cafe**, lobby floor<br>JW Marriott Phuket resort |
| 10:00-10:10 | Intro & greetings | **Mai Khao Ballroom**<br>JW Marriott Phuket resort |

### Session 1: You Have Chosen... Wisely. Moderator: Costin Raiu

| | | | |
|---|---|---|---|
| 10:10-10:30 | Marking for Protection: Digitalizing the Red Cross Emblem | **Mauro Vignati**, International Committee of the Red Cross | As societies undergo digital transformation, the use of cyber operations in armed conflicts is on the rise, prompting the International Committee of the Red Cross (ICRC) to consider adapting their iconic Red Cross, Red Crescent, and Red Crystal emblems for the digital realm, creating a 'digital emblem.' This concept aims to protect designated digital assets in much the same way as physical assets have been safeguarded for over a century. In this talk, the ICRC explores the advantages, risks, and challenges while assessing different technical solutions to pave the way forward. |
| 10:30-10:50 | StripedFly: Traversing the Blue Expanse in Search of Eternal Wonders | **Sergey Belov**, Principal Security Researcher, GReAT, Kaspersky<br>**Sergey Lozhkin**, Principal Security Researcher, GReAT, Kaspersky | Last year, we uncovered a long-standing and elusive APT that had been operating in the wild for several years, utilizing a modular framework supporting both Linux and Windows. This APT cleverly integrated a TOR client with a hidden C2 server within the TOR network and leveraged legitimate web services like GitLab, GitHub, and Bitbucket for its operations. Despite initially being mistaken for a Monero miner, a deeper investigation revealed its persistence since 2017, likely linked to the Equation malware, and its global reach, infecting over a million new victims by June 2022. However, it has since waned, potentially due to heightened scrutiny and the discontinuation of the insecure SMBv1 protocol. |
| 10:50-11:10 | Unearthing Cyber Threat Treasures: Malstream's Quest in the Digital Wilderness | **Matteo Corradini**, Lead Cyber Threat Intelligence Engineer, Cluster25 | Malstream is an innovative framework for automating malware attribution, using popular detection rules like YARA, Suricata, and Sigma. It can handle large volumes of malware samples, making it a valuable tool for CTI analysts to streamline attribution tasks and focus on manual reverse engineering for critical artifacts. It's adaptable for use in CSIRTs, CERTs, or SOCs, facilitating large-scale attribution by collecting and analyzing samples from various sources, enriching data, and offering an intuitive GUI for rule management. The system includes connectors for data ingestion, a backend with dynamic and static analysis modules, and a frontend for result and rule management, all designed for efficient and scalable malware analysis. |
| 11:10-11:30 | Large Language Models against the Kingdom of Phishers | **Eduard Alles**, Virus Analyst, G Data CyberDefense | In the past year, concerns about the cybersecurity threat posed by large language models like OpenAI's GPT have grown due to the potential for attackers to use AI for more proficient malware creation and social engineering attacks, leading to an anticipated increase in phishing attempts. Phishing websites, which are easily created, prompt a need for accelerated analysis and classification. Our research focuses on using machine learning and large language models, achieving a high F1 Score of 0.92 with a 90% phishing certainty threshold, providing an efficient and cost-effective solution for identifying and blocking phishing sites, even as attackers change tactics or targets. |
| 11:30-11:50 | Unleashing the Secrets: A Full Analysis for the Complex LODEINFO v0.7.1 | **Suguru Ishimaru**, ITOCHU Cyber & Intelligence Inc. | In this session, I delve into my extensive research on a sophisticated APT campaign utilizing the elusive LODEINFO backdoor. Despite limited open-source information, LODEINFO's intricate modules feature numerous anti-reversing measures. Maintaining robust analysis capabilities is vital in fulfilling our CSIRT responsibilities and safeguarding our organization.<br>This presentation unveils the outcomes of a comprehensive analysis of LODEINFO's latest version, v0.7.1. Gain insights into its backdoor modules, propagation methods, and underlying infrastructure. Join me in unraveling the complexities of this potent threat. |
| 11:50-12:10 | Coffee break | | **Mai Khao Ballroom prefunction area**<br>JW Marriott Phuket resort |

## Session 2: Signal Detected... Moderator: **Jeffrey Esposito**

| | | | |
|---|---|---|---|
| 12:10-13:00 | Securing Supply Chains in the Open Source Era. Panel Discussion<br>Moderator: **Genie Gan**, Head of Public Affairs, APAC & META, Kaspersky | **Craig Jones,** Director, Cybercrime Directorate INTERPOL, Singapore<br>**Major General Teerawut Wittayakorn**, Deputy Secretary-General, National Cyber Security Agency, Thailand<br>**Vladimir Radunović**, Director of Cybersecurity & E-diplomacy, DiploFoundation, Serbia<br>**Ron Brash**, VP of Technical Research & Integrations, aDolus Technology Inc, Canada<br>**Anton Ivanov**, Chief Technology Officer, Kaspersky | |
| 13:00-13:40 | **PechaKucha** | | |
| | Neuro-Hacking Unleashed: Decrypting Personality for Cybersecurity Excellence | **Natalia Antonova**, Exponential Coach | |
| | Dropping Elephant Never Dropped | **Jin Ye (Seth)**, Senior Security Researcher, GReAT, Kaspersky | |
| | A Multi-View Graph Learning Approach for Host-based Malicious Behavior Detection | **Wu Tiejun**, Head of Fuying Laboratory, NSFOCUS | |
| | The Cyber Jungle Expedition: Navigating Supply Chain Attacks | **Hassan Khan Yusufzai**, Security Researcher | |
| | Your First Dive into the IoT Research | **Vitaly Kamluk**, Head of APAC Unit, GReAT, Kaspersky | |
| 13:40-13:40 | Lunch | | **JW cafe**, lobby floor<br>JW Marriott Phuket resort |

## Session 3: Into the Cyberjungles... Moderator: **Margarita Khrapova**

| | | | |
|---|---|---|---|
| 14:40-15:00 | How Many Gates to the Temple of Space? Shapes of Tunnels Drilled by Desecrators | **Askar Dyussekeyev**, Head of the Malicious Code Research Center, State Technical Service, KZ-CERT | In July of this year, one of the Kazakh space telecommunications operators turned to the National Computer Emergency Response Team (KZ-CERT) with a request to provide assistance in neutralizing a complex cyber attack. The investigation revealed an Advanced Persistent Threat (APT) that had infiltrated the operator's infrastructure for several years. The attack involved a wide array of tools, including exploits on Microsoft Exchange, web shells, a custom "mimilib" library for privilege escalation, and the use of the "PlugX" malware. Additionally, the attackers employed various tactics to evade detection, making it challenging to respond effectively to the cybersecurity incident. |
| 15:00-15:20 | He's not a Simple MSI. Hunting and Protecting Against Privilege Escalation in MSI | **Nikita Kurganov**, Senior Fintech SOC Engineer, Yandex | In 2023, Yandex hosted a pentest in which the pentesters successfully increased privileges on a secure terminal server on windows through a newly discovered feature of Windows in the MSI installer. This report will examine this feature in MSI and suggest various ways to detect attempts to escalate privileges through this attack vector using various information security tools |
| 15:20-15:40 | USB flows in the Great River: Solving Unnoticed Long-term APT RAT Puzzle | **Hiroshi Takeuchi**, Security Researcher, MACNICA | Overseas offices often have less mature security measures than headquarters due to cultural and governance differences, with internet-facing devices becoming prime targets. While vulnerabilities and zero-day attacks on these devices are significant threats, USB devices are also a major attack vector in the APAC region. Specifically, we'll delve into the activities of TA410, focusing on their use of USB devices in a campaign we're tracking as "Operation USBFlowing." We'll examine FlowCloud, a toolset used by TA410, including its latest version (v6.0.0 from March 2023), which poses challenges for analysts due to its code complexity. We'll also profile FlowCloud's developers and discuss TA410's evolving tactics, emphasizing the importance of addressing both old and new threats. |
| 15:40-16:00 | Space Pirates: Raiders of Privacy | **Denis Kuvshinov**, Head of Threat Intelligence Department, Positive Technologies | In late 2019, the Positive Technologies Expert Security Center (PT ESC) uncovered the Space Pirates cybercrime group, active since at least 2017. In early 2022, the first comprehensive research on this group emerged. Over the past year, Space Pirates intensified attacks on Russian companies, targeting government institutions, educational organizations, security firms, aerospace manufacturers, and more. They primarily employ the Deed RAT, an evolution of ShadowPad and PlugX, which appears exclusive to them and is continuously evolving. Additionally, they were linked to a new malware called Voidoor, utilizing Github and voidtools.com as C&C servers, with login events tying it to the Space Pirates group. |
| 16:00-16:20 | Unearthing TetrisPhantom: Discovering Secrets of an Intricate Cyber Threat Campaign | **Noushin Shabab**, Senior Security Researcher, GReAT, Kaspersky | Early in 2023, Kaspersky uncovered an ongoing sophisticated attack on government entities in the APAC region, exploiting secure USB drives with hardware encryption. These drives, used for secure data storage and transfer, were compromised, revealing a long-standing campaign involving malware modules for command execution and data collection. The attack employed advanced techniques like virtualization-based obfuscation, direct SCSI communication with USB drives, self-replication through connected drives, and code injection into access management software. This highly targeted and limited attack suggests a skilled and resourceful threat actor focused on espionage in sensitive government networks, emphasizing the need to understand their tactics and prepare for future attacks. In this talk we will look at the the technical details of the malicious files involved in these attacks. |
| 16:20-16:40 | Coffee break | | |

## Session 4: The Last Revelation

Moderator: **Dmitry Galov**

| | | | |
|---|---|---|---|
| 16:40-17:00 | Operation Triangulation: Connecting the Dots | **Igor Kuznetsov**, Director, Global Research & Analysis Team, GReAT, Kaspersky | Zero-day, zero-click, kernel exploit, iOS spyware, targeted attack – each of these words separately can get a security researcher excited. Now imagine discovering them all, one by one, in your own network, within a hand's reach, on the mobile devices of your co-workers. At Kaspersky, we call it Operation Triangulation. In this talk we will tell the story of our discovery, how starting with just a network anomaly it was possible to reconstruct all the stages of a complicated targeted attack. Then, we will describe its components, including a zero-click exploit chain, and a modular APT platform. We will discuss the challenges we encountered during the research, and the tools and techiques that we used to overcome them. |
| 17:00-17:20 | APT Patchwork 's "Herminister operation" | **Desmond Dai**, Manager, Knownsec APT TI team<br>**Bohang Mo**, Malware Analysis Engineer, Knownsec APT TI team | In 2022, Knownsec's APT TI team uncovered an attack campaign linked to APT Patchwork, which we've named "Herminister operation" after one of its weapons. This operation employs undisclosed weapons not previously known to the cybersecurity community. Patchwork utilizes numerous open-source red team tools and modifies free tools. We also detected strings associated with the Confucius APT team in Herminister, suggesting shared resources among South Asian APT groups. The arsenal comprises multiple attack chains, encompassing functions like information gathering, UAC bypass, lateral movement, network propagation, deployment, RATs, keyloggers, and screen capture tools, totaling 76 weapons. Our presentation will will focus on sharing the arsenal, techniques and tactics of the "Herbminister operation". |
| 17:20-17:40 | Fodcha Botnet, Would You Mind Surrendering Once More? | **Alex Turing**, Senior Security Expert, QAX | When discussing the DDoS landscape, the Mirai botnet is often a central focus. Since its source code leaked in 2016, it has driven a surge of interest in DDoS attacks, although most attempts by script kiddies ended in failure. However, the Fodcha botnet emerged as an exception in January 2022 and remained active until April 2023, an impressive 15 months. Fodcha boasted over 780 members in its Telegram group, with over 35,000 daily active bot nodes and 40+ IP-bound C&C domains capable of launching massive attacks exceeding 1Tbps. The botnet targeted over 100 victims daily, accumulating more than 30,000 targets, with a single day reaching 1,396 attacks. Our data collection and analysis, including the discovery of Fodcha's C&C source code, contributed to its shutdown in April 2023, showcasing the importance of DDoS research for better detection and mitigation. |
| 17:40-18:00 | A Cascade of Compromise: Unveiling Lazarus' Campaign Exploiting Security Company Products and its Intricate Connections with Other Campaigns | **Seongsu Park**, Lead Security Researcher, GReAT, Kaspersky | The Lazarus Group, a notorious cyber threat actor, has focused on a South Korean software vendor for an extended period, aiming to steal source code and exploit the software's supply chain. They developed a method to use this software for spreading their malware and expanded their tactics to strike another South Korean vendor. Our investigations unveiled a sophisticated malware launched in memory after exploiting stolen vulnerabilities. This covert approach fetches and executes malware from a remote server without touching the disk, utilizing techniques like DLL side-loading and obfuscation. Their global targeting indicates a widening presence, underscoring the geopolitical implications of their activities and emphasizing their advanced expertise. This research provides insights into Lazarus Group's tactics and worldwide presence, empowering the security community to bolster defenses against this highly sophisticated threat actor. |
| 18:00-18:20 | Surprise Keynote | | |
| 18:20-18:30 | Wrap up | | |
| 19:15-19:30 | Transfers to Dinner | | |
| 20:00-23:00 | Thai Style Burlesque Dinner & Awards | | **Junkyard Theater Phuket**<br>49/6 Moo. 5, Chalermphrakiat, Ror 9 Road, Rasada, Muang Phuket, 83000 |

## October 27th

| | | |
|---|---|---|
| 07:00-09:30 | Breakfast | **JW cafe**, lobby floor |
| 10:00-17:00 | Activity program / Business Track | |
| 19:30-22:00 | Farewell dinner | **M Beach club**<br>JW Marriott Phuket resort |

## October 28th

| | | |
|---|---|---|
| 07:00-11:00 | Breakfast | **JW cafe**, lobby floor |
| All day | Departures | |