OFFZONE 2024

August 22–23, Moscow
ZIL cultural center

August 22, Thursday — Main track

10:00–10:30

Opening ceremony

Language: Russian

10:30–11:30

Keynote address
rOO+ Of 3/\@

Sergey Golovanov
Chief Security Expert, Kaspersky

The presentation covers a range of security incidents that have occurred over the last 20 years. We will look into their root causes and analyze some facts that typically escape the public eye

Language: Russian   Difficulty level: easy

11:30–12:30

Gone in five SMS: a story about RCE in Telit's modems

Alexander Kozlov
Principal Security Researcher, Kaspersky

Sergey Anufrienko
Group Manager, Kaspersky

In 2023, Kaspersky's researchers discovered several vulnerabilities in a family of modems manufactured by Telit. If exploited, these flaws could lead to the complete compromise of the modems.

In the Telit firmware, the researchers found a heap overflow vulnerability in the SUPL message handler. This vulnerability allowed for the remote execution of arbitrary code on the modem just by sending a few text messages.

Another group of security issues was identified in the Telit MIDlets. Research showed that it is possible to bypass the digital signature verification for both user and manufacturer MIDlets, as well as escalate the privileges of any user MIDlet to the manufacturer's level.

As a full proof of concept (PoC), the researchers developed their own driver that accepts commands via SMS and installed it on the modem through the vulnerability in the SUPL message handler. This enabled them to remotely activate over-the-air provisioning (OTAP) and install a non-Telit MIDlet with manufacturer privileges

Language: Russian   Difficulty level: hard

12:30–13:30

Pentesting FreeIPA, or Delving deeper into the zoo

Mikhail Sukhov
Head of Security Assessment, Angara Security

FreeIPA is becoming increasingly common in infrastructures. The speaker invites the audience to dig into the innards of FreeIPA and find out where vulnerabilities might be hiding

Language: Russian Difficulty level: hard

13:30–14:30

[Dev]iceSecOps, or Why we wrote a tool to analyze firmware

Boris Ryutin
Security Engineer, Yandex

Nikita Lychanyi
Security Engineer, Yandex

After switching to the defender side, their love for device hacking didn't let them go, so they decided to reuse their skills to improve device security. This is how the YA4FW (Yet Another Analyzer for Firmwares) tool was born

Language: Russian Difficulty level: medium

14:30–15:30

Malware and hunting for persistence: how do adversaries hack your Windows?

Zhassulan Zhussupov
Co-founder, MSSP Research Lab

Zhassulan will share the story of how he discovered several non-standard and unusual methods for malware persistence using the registry modifications and DLL hijacking vulnerability in Windows Internet Explorer, Win32API Cryptography, Windows Troubleshooting, Microsoft Teams (fixed in 2024), and Process Hacker 2 (fixed in v3)

Language: Russian Difficulty level: medium

15:30–16:30

Binary software composition analysis in action: searching for vulnerable native libraries in Android apps

Evgeny Zhukovsky
Security Researcher, Founder, DAP Solutions

Similarly to most other applications, mobile ones use open source components (OSS). But how carefully do developers check the versions of libraries they use for known vulnerabilities?

To identify and track third-party dependencies in products, there are compositional analysis tools (SCA). However, what to do if you do not have the source code of the application or its parts?

Using the analysis of native Anrdoid application libraries as an example, the speaker will explore the implementation of binary compositional analysis (BSCA) and the tasks addressed by it. He will also share the things he found in the dependencies of popular Russian mobile applications

Language: Russian Difficulty level: hard

16:30–17:30

Red team chronicles: Wi-Fi, 0-day, and more

Denis Pogonin
Senior Application Security Expert, BI.ZONE

The speaker will discuss exploitable vulnerabilities and attack vectors used in red team projects. He will cover attack chains for gaining initial access via web application vulnerabilities, phishing, and Wi-Fi. Denis will also demonstrate the search for 0-day vulnerabilities in the Websoft HCM application and ways to further develop attacks via the TeamCity tool

Language: Russian Difficulty level: medium

17:30–18:30

May 2024 attacks in Russia: pros or script kiddies?

Ivan Syukhin
Head of Incident Response Group, Solar

While the whole country seemed to be busy barbecuing throughout the first half of May, Ivan's team was busy responding to incidents. He will talk about three most notable attacks.

The first attack was carried out by a well-known group armed with ngrok, gs-netcat, and LockBit 3.0. The speaker will analyze some of the attackers' tools and actions to demonstrate that sometimes the group's operators were not as savvy as one might expect.

In the second attack, the allegedly pro-Ukrainian group tried to destroy the victim's infrastructure (host encryption, data deletion, ESXI destruction). Ivan will examine the adversaries' tools that include the localtonet utility and the SOGFN.sys driver for bypassing anti-malware mechanisms.

The third attack was orchestrated by the Shedding Zmiy group. Ivan will share his observations on changes in the tactics and techniques of the group as compared to its previous attacks.

In all of the attacks, despite the difficulties, Ivan's team was able to restore the initial access point, and he will elaborate on how it was achieved

Language: Russian Difficulty level: easy

August 22, Thursday Community track

11:30–12:30

Red team: using Google against itself

Alexander Goncharov
Senior Security Analyst, Innostage

In recent years, Google has made life difficult for the makers of phishing websites, and rightly so. However, penetration testers also find themselves affected by these changes.

In this talk, Alexander will explore how to use OSINT and Google’s source code leaks to overcome Google's limitations. He will examine the methods for bypassing sandboxes, red pages, and Google's other protective mechanisms that are not easily recognized by the average user. Additionally, Alexander will discuss practices employed by top red teams

Language: Russian Difficulty level: medium

12:30–13:30

Underground circus: arbitration on the darknet

Alexander Zabrovsky
Digital Footprint Analyst, Kaspersky

This presentation will unveil the inner workings of darknet forums, exploring their structure, audience, and the intricacies of cybercriminal activities, including how members scam each other. The speaker will dissect the entire underground market system—from forum rules and the role of escrow services (specialized “protection” services) to the nuances of the reputation system and the workings of their “courts” (arbitrages).

Alexander will examine numerous real-life cases, ranging from failed deals to amusing conflicts between users, and study how the arbitrators resolve the most controversial or humorous disputes. Prepare for surprising and incredible stories that demonstrate even the shadow network isn’t devoid of humor and drama.

This talk is beneficial for anyone interested in the topic, especially for OSINT specialists, cybersecurity and darknet researchers, and employees of specialized departments dealing with digital risk protection, antifraud, and threat intelligence

Language: Russian   Difficulty level: easy

13:30–14:30

A story of one vulnerability: an RCE in telecom hardware

Alexey Romanov
Head of Cloud Cybersecurity R&D, BI.ZONE

Starting with 2022, many Russian companies had to search for alternatives to international vendors' software. This change brought to life a large number of locally designed applications and appliances.

An influx of new hardware and software gave rise to more cybersecurity risks as fresh-out-of-the-oven solutions tend to have numerous flaws and vulnerabilities.

Alexey will share a story of a vulnerability that was discovered in the firmware of some Russian telecom equipment. The vulnerability enabled unauthenticated users to execute unauthorized code

Language: Russian   Difficulty level: medium

14:30–15:30

Developing EDR evasion strategies

Kirill Komogorov
Pentester, BI.ZONE

Kirill will cover the basics of the architectural structure of EDR systems. He will look at EDR solutions in the context of Windows operating systems. The main components of EDR will be examined both from the attacker's and the defender's points of view to demonstrate approaches to bypassing EDR and ways to counter such efforts

Language: Russian Difficulty level: hard

15:30–16:30

Hiding in AI: malicious code detection in ML models

Tatiana Kurmasheva
Founder, AI Security Technologies LLC

In this talk, Tatiana will focus on the detection of malicious code in machine learning models. She will talk about the structure of file formats used for storing such models, the process of running them, and the existing attack vectors. The speaker will also present the results of a study on popular community repositories

Language: Russian Difficulty level: medium

16:30–17:00

Crash report accumulation during continuous fuzzing with CASR

Ilya Yegorov
DevOps Engineer, SberTech

Continuous fuzzing often results in crashes that are similar to or duplicating old ones. CASR provides a method to automatically discard duplicates and detect similar crashes

Language: Russian Difficulty level: hard

17:00–18:00

PCI-exploit

Egor Koleda
Hardware security researcher, 0x08

A look at DMA attacks and how to organize one at a low cost by finding vulnerabilities in hardware

Language: Russian Difficulty level: medium

August 22, Thursday AppSec.Zone

12:30–14:00

BI.ZONE Bug Bounty: progress report

Evgeny Voloshin
Head of Security Assessment and Antifraud, BI.ZONE

Andrey Levkin
Product Owner, BI.ZONE Bug Bounty

Sergey Krainov
Head of Cybersecurity Expertise, Sber

Roman Mylitsyn
Head of Research and Innovation, Astra Group

Artem Belchenko
Independent researcher

Many Russian companies have already appreciated bug bounty as an effective tool for analyzing the security of the external perimeter. Major organizations from the finance, government, IT, retail, and other industries are increasingly bringing their programs to platforms. The experts will discuss the development of the bug bounty market in Russia and share the progress of the BI.ZONE Bug Bounty platform

Language: Russian

15:00–16:00

Bug bounty: simple critical bugs

Alexey Lyamkin
Bug Bounty Expert, VK

The speaker will discuss how business-critical threats may emerge from minor errors

Language: Russian   Difficulty level: medium

16:00–17:00

Playing with fire, or Burnout as a trend of the cybersecurity industry

Sergey Zybnev
Pentester, Awillix

Artem Belchenko
Independent researcher

What is burnout? Where does it come from? Why do we burn out so often? Can we do anything about it? Sergey and Artem will answer these questions and more

Language: Russian   Difficulty level: easy

17:00–18:00

A platform for automating fuzzing processes: problems and solutions

Victoria Egorova
Deputy Head of Security Analysis Department, Astra Group

Alexey Panov
Dynamic Analysis Team Lead, Astra Group

Everyone knows that fuzzing is a necessary stage of security analysis for any product. When you have one small application in front of you, there are no difficulties to fuzz it, but what if we are talking about an operating system?

The speakers will share why they came to the conclusion that they need their own platform for automating fuzzing processes. Victoria and Alexey will also cover the existing platforms and the situations when these platforms are not enough

Language: Russian   Difficulty level: hard

18:00–18:30

How SCA tools generate false positives

Alexey Moskvin
Independent security researcher

Daniil Sadyrin
Independent security researcher

The speakers will discuss why achieving the overall project security requires taking a snapshot of software components and their vulnerabilities in addition to assessing each component individually

Language: Russian   Difficulty level: medium

August 22, Thursday   AntiFraud.Zone

11:50–12:30

Fraud in the trucking industry: nominee directors

Farid Jafarov
Logistics Security Association

Freight transportation is a critical industry without which no state exists. Fraudsters know this and are trying in every possible way to take possession of other people's property. The talk will focus on a type of fraud that has touched logistics, and specifically road freight transportation. Why is the number of nominee directors on the rise and what are the consequences for the industry? Farid will offer his answers to these questions

Language: Russian   Difficulty level: easy

12:30–13:15

How pictures on the Internet take your money and data

Sergey Bnyatov
Head of SOC and Incident Response Team, Ecom.tech
(ex Samokat.tech)

The speaker invites you to think about digital risk monitoring—about what it is and why it is important. How do digital risks expand the potential attack surface and how can knowing what's going on around your brand help you? Why does the SOC need this information? How to build your own data model for brand monitoring and verification while using nothing but your laptop and some Python?

Language: Russian   Difficulty level: hard

13:15–13:45

The state of fraud and what to expect next

Aleksandr Bolshunov
Lead Expert, Sberbank

Aleksandr will examine popular fraud schemes encountered by companies and individuals this year. How do cybercriminals use generative AI and what digital footprints should you look out for? Why does the FakeBoss scheme still work and how to handle it all?

Language: Russian Difficulty level: medium

13:45–14:30

Sber's experience in leveraging deep learning for antifraud purposes

Kirill Vyshegorodtsev
Executive Director, Cybersecurity Research Laboratory, Sber

Andrey Pinchuk
Head of AI Modeling and Development, Antifraud Department, Sber

Gradient boosting has been the state-of-the-art technique in antifraud solutions for years. But can the results be significantly improved with the same data sources?

The talk is devoted to the latest research on the application of deep learning technologies in antifraud

Language: Russian Difficulty level: hard

14:30–15:15

Jeez, scammers are here again! How to build an antifraud system from scratch?

Katya Turing
Antifraud specialist

The speaker will present a company case study demonstrating how to assess the damage from scammers and launch an effective antifraud system

Language: Russian Difficulty level: medium

15:45–16:15

A new round of Buhtrap: a scheme with web injection

Andrew Mansurov
Senior Fraud Prevention Analyst, BI.ZONE

In his talk, Andrew will explore the activities of the financially motivated cybercriminal group Buhtrap and analyze in detail a new scheme with web injection. The scheme helped the adversaries find a new way of stealing money from Russian organizations

Language: Russian Difficulty level: hard

16:15–17:00

Telco fraud

Petr Alferov
Director for Fraud Management and Revenue Assurance, Beeline

The speaker will focus on the sources of fraudulent traffic and the development of antifraud solutions in the telecommunications industry

Language: Russian Difficulty level: medium

17:00–17:30

Backstreet ploys: Who commits loyalty program fraud and how they do it

Vera Kolenikova
High-Tech Crimes Investigations Department Specialist, F.A.C.C.T.

Vera will give an overview of the black market for loyalty program points. She will talk about bonus card dumps, refreshable barcodes, unauthorized access to loyalty program processing systems and offer her insight on what can be done about it (and a little bit on who is to blame for the current situation)

Language: Russian Difficulty level: hard

17:30–17:50

No pasaran? Bots: incessant battles on the shadow frontlines

Dmitry Krikov
Chief Technology Officer, NGENIX

For a typical online marketplace, bot traffic can amount up to 90% of the total web traffic. The so-called intelligent bots, such as parsers, scrapers, scalpers, and others can be a real headache for IT and web security professionals. Malicious bot traffic results in an extra burden on the IT infrastructure, excessive costs and losses, and additional security threats. Bad bots simulate real web user behavior to evade security systems, and even security professionals struggle to identify them. In his presentation, Dmitry will cover various methods of bot identification and complex bot attacks mitigation based on real-life experience. This topic might be of interest for web IT and security specialists

Language: Russian   Difficulty level: medium

17:50–18:10

Loan pyramid schemes: a new trend or a well-forgotten one

Madina Azhakhmetova
Executive Director for Security Investigations, Sberbank

The speaker believes that all actors of the financial market face a new challenge in the fight against external fraud. And the financial pyramid is an example of external fraud that hurts ordinary people who do not realize the consequences of their actions. This leads to fatal mistakes and, as a result, can take many different forms and amounts of liability.

Madina will give concrete examples and share some of Sber's approaches to countering fraud

Language: Russian   Difficulty level: medium

18:10–18:30

How our system identifies and processes fake reviews

Andrei Budilov
Head of Antifraud Group, Yandex

In this talk, the speaker will dive into why people post fake reviews on different platforms. He'll look at how this hurts both the platforms and their users. He'll also cover the key metrics for measuring antifraud success and explore some AI techniques employed by Yandex to spot fake reviews

Language: Russian   Difficulty level: medium

August 22, Thursday   CTF track

11:30–12:00

CTF and life

Pavel Blinnikov
Head of Vulnerability Research, BI.ZONE

Outside observers complain that the tasks included in CTF competitions are often "unrealistic".

In the opening talk of the CTF track, Pavel will present his view on the competitions vs. real life problem. He will share how the skills gained at CTF can be useful in day-to-day situations

Language: Russian   Difficulty level: easy

12:00–12:30

Multipurpose CTF: using the task concept outside of competitive CTF

George Zaitsev
Reverse Engineer, Positive Technologies

George will share his vision of the CTF task concept, which can be used outside of the competitive CTF format

Language: Russian   Difficulty level: easy

12:30–13:00

Exploiting browser security

Yuriy Pazdnikov
Junior Pentester, BI.ZONE

The speaker will discuss initial steps required to exploit browser security vulnerabilities. He will share some practical insights he gained in CTF competitions

Language: Russian Difficulty level: medium

14:00–15:00

Why you don't have to be afraid of lattice-based cryptography

Alexander Sokolov
Junior Security Consultant, Aztec Labs

Kirill Kudryavtsev
Neplox audit group

The speakers will explain the basics of lattice-based cryptography and discuss the LLL algorithm and its use cases in cryptanalysis. They will also give an overview of approaches to lattice construction and analyze some non-obvious examples from CTFs

Language: Russian Difficulty level: hard

15:00–16:00

Hacking techniques at the service of a security engineer v1.1

Artem Artamonov
Security Vision

As an engineer in IT, and especially in information security, Artem has encountered numerous situations where deadlines are tight, the project needs to be completed, but the infrastructure is almost entirely locked down, and the bureaucracy, people, regulations, and who knows what else prevent you from getting the job done. He had to get creative and use borderline hacking techniques to bypass such restrictions. These are the stories he will share in his talk. Version 1.1, enriched

Language: Russian Difficulty level: easy

August 22, Thursday **AI.Zone**

11:30–12:20

Self-hosted LLMs in cybersecurity

Dmitrii Lekomtsev
Senior Machine Learning and Data Research Specialist, BI.ZONE

The speaker will discuss the advantages of local large language models (LLMs) over popular online services. The issues of model selection, estimation and reduction of training costs, as well as new risks associated with the use of LLMs will be addressed. The speaker will demonstrate an AI assistant based on a self-hosted LLM and incorporated into BI.ZONE EDR

Language: Russian Difficulty level: medium

12:20–12:40

How to use the full power of ChatGPT without fear of data leaks

Aleksandr Smirnov
Senior Application Security Engineer, Cian

In this talk, Aleksandr will show how Cian development team implemented a secure, reliable, and extensible tool for enabling employees and services to interact with external LLMs (such as ChatGPT). The discussion will cover how his team gained control over the integration process, data transmission, and available limits. Additionally, Aleksandr will explore the challenges and benefits of the implementation

Language: Russian Difficulty level: medium

12:40–13:10

Few-shot prompting in SOC

Igor Gots
Security Engineer, Yandex

Can the few-shot prompting technique help us evaluate the SIEM response?

Language: Russian Difficulty level: easy

13:10–13:30

Threat intel with LLM for LLM

Yuriy Lebedinskiy
Leading Expert, Sberbank

To keep up to date with the latest vulnerabilities of systems that use generative AI, cybersecurity specialists have to study lots of scientific publications and news.

In his presentation, Yuriy will explain why "you can't just take and use" large language models to select scientific articles. He will present the concept of an ideal threat intelligence system and talk about his publication tracking system, which can be used for selecting articles on AI cybersecurity and other topics

Language: Russian Difficulty level: medium

13:30–14:35

Generative and multimodal models to detect and classify phishing websites

Yuri Ivanov
Technical Director, Head of ML, AV Soft

Vladimir Larkin
ML Engineer, AV Soft

Yan Tokarev
ML Engineer, AV Soft

The presentation covers modern methods for detecting phishing websites and protecting brands. It focuses on two main areas: semantic search for new phishing sites using generative models and large language models (LLMs), and multimodal detection of phishing links, which includes visual analysis, content analysis, and linguistic analysis of URL pages.

The process of generating semantic queries for adaptive phishing site detection is explained, emphasizing both the semantics and context of attacks. Special attention is given to natural language processing (NLP) and computer vision (CV) technologies.

The presentation outlines the model architectures, training specifics, effectiveness metrics, and overall system functionality. Real-world examples of how these methods have been successfully applied to protect brands and prevent cyberattacks are provided. The presentation concludes with key takeaways, a demonstration of the system in action, and recommendations for implementation

Language: Russian Difficulty level: medium

14:35–15:15

More data is required: predicting CVE metrics by their mutual transformation

Dmitry Levshun
Senior Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences

This presentation contains a study of the effectiveness of EL and DL methods in the task of predicting CVSS metrics based on their mutual transformation. The uniqueness of the solution lies in the use of CVSS v3 metrics to predict CVSS v2 metrics and vice versa.

In his talk, Dmitry will explore the collected datasets and the results obtained for predicting each of the metrics. He will also discuss the challenges he encountered and ways to address them

Language: Russian

Difficulty level: hard

15:15–16:10

Your face looks familiar to me: intelligence, analysis, and attacks on ML in face recognition systems

Alexander Migutsky
ML Security Researcher, Positive Technologies

We live in a world where facial recognition systems are used almost everywhere, from age validation and online biometric identification to video surveillance and POS payment. Not surprisingly, the machine learning algorithms used in these systems have improved in leaps and bounds in the last 10 years. In this talk, the speaker will give an overview of facial recognition technologies, attacks and circumvention techniques, and demonstrate two new attacks targeting online and offline recognition systems. These attacks have been successfully applied to existing commercial and open-source facial recognition systems

Language: Russian

Difficulty level: hard

16:10–16:50

Poisoned docs: how to attack RAG pipelines

Vladislav Tushkanov
Kaspersky MLTech Group Manager, Kaspersky

Retrieval-Augmented Generation (RAG) is the major paradigm for developing LLM-based applications that work with large texts. However, a significant part of LLM systems is vulnerable to indirect prompt injection attacks, where external unverified data includes malicious instructions. How easy is it to trick a RAG system into executing unintended instructions with a malicious document? Using ChatGPT as an example, the speaker will look at several techniques that make such attacks effective

Language: Russian Difficulty level: medium

16:50–17:30

LLM tRAGedy. How to exploit backdoors in a RAG knowledge base

Artyom Bulgakov
Pentester, BI.ZONE

Ruslan Makhmudov
Security Assessment Specialist, BI.ZONE

Artyom and Ruslan will talk about the RAG architecture in LLM, the main vectors of attacks through malicious documents, and ways to optimize such attacks

Language: Russian Difficulty level: medium

17:30–18:10

Data poisoning in LLMs and new risks in multi-agent systems

Danil Kapustin
AI Engineer, Raft Digital Solutions

This talk addresses the current security challenges in large language models (LLMs) and multi-agent systems. The speaker will discuss key threats leading to data poisoning. He will also explore how excessive autonomy in AI can introduce new vulnerabilities and will suggest strategies for mitigating these risks

Language: Russian Difficulty level: easy

18:10–18:30

Pentest Copilot, or How I created an AI pentest assistant

Danila Urvantsev
Security Analysis Specialist, USSC

The talk will examine what can be achieved by uploading expert materials to an LLM knowledge base

Language: Russian

Difficulty level: easy

August 23, Friday — Main track

11:00–12:00

Security of binary applications in Yandex

Pavel Cheremushkin
Senior Information Security Engineer, Yandex

High-performance software is often written in memory unsafe languages like C and C++. In Yandex, many solutions are being developed in C++. Some of them are available exclusively to internal teams and some are in open source (e.g., YDB, YT, userver). Pavel will talk about his team's approaches to ensuring the security of such services and experiments in automating the search for vulnerabilities using fuzzing. He will also cover the most interesting vulnerabilities identified in internal audits and submitted to Yandex by bug hunters

Language: Russian

Difficulty level: medium

12:00–13:00

Container escapes: Kubernetes 2024 edition

Dmitry Evdokimov
Founder & CTO, Luntry

Nickolai Panchenko
Senior K8s and Cloud Security Specialist, T-Bank

Container escapes in K8s have been addressed before. The evolution of the ecosystem and IT tools create new opportunities. But those, as we all know, breed new vulnerabilities. In the K8s infrastructure, it becomes possible to exploit new attack vectors to escape from the container. At the same time, the old vectors are still there to remind us about themselves. The speakers will look at examples of escape vectors that are worth knowing and keeping in mind in 2024

Language: Russian   Difficulty level: medium

13:00–14:00

Filtering eBPF in Kubernetes, or Paddling down the treacherous river of network data

Alexey Rybalko
Container Security Specialist, Kaspersky

Technologies for filtering network data flows in a containerized environment are a must-have for protection against intrusion.

Several approaches are used to intercept and analyze data. Among them are the implementation of service mesh, service sidecar containers in Kubernetes Pod, and the implementation of protection agents in containers. All such approaches take a significant percentage of cluster resources, since each container with payload needs an accompanying sidecar or agent.

A lighter and faster approach involves a centralized session connection request checking in the Linux kernel on the Kubernetes node using eBPF technology. However, opting for this approach implies overcoming some challenges.

The speaker will share how his team navigated the river of network data and finally made a deep-water hunt and tamed eBPF.

The presentation will be useful for anyone who plans to dive into the topic of Kubernetes security (i.e., literally for everyone), as well as for sympathizers on the shore

Language: Russian   Difficulty level: medium

14:00–15:00

Hunting Red List ToddyCat

Natalya Shornikova
Lead Cyber Threat Intelligence Analyst, Kaspersky

Andrey Gunkin
Senior Malware Analyst, Kaspersky

The speakers will discuss the APT group ToddyCat and its espionage attacks against government organizations in Southeast Asia and Eastern Europe. The talk will include a detailed overview of the tools used by the group

Language: Russian Difficulty level: hard

15:00–16:00

Storm clouds: incident investigations in cloud infrastructures

Anton Stepanov
Lead Computer Forensics Specialist, BI.ZONE

Anton will share his experience of cloud infrastructure investigations.

The trend of the season is trusted relationship attacks. But what if an attacker targets a cloud service provider to gain access to client administration consoles or hypervisors? In this case, the task of accessing client data becomes significantly easier. The DFIR team at BI.ZONE investigated several cases where cloud service providers were compromised. The talk will cover these investigations, their bottlenecks and challenges. Anton will also share an investigator's perspective on how to detect such attacks and what cloud provider clients can do to reduce the risk of compromise

Language: Russian Difficulty level: medium

16:00–17:00

V8 sandbox bypass

Yuriy Pazdnikov
Junior Pentester, BI.ZONE

The V8 sandbox is a new mechanism designed to protect the JavaScript engine in Chromium-like browsers. In his talk, Yuriy will describe a way to bypass the sandbox using the vulnerability he discovered. He will also examine a new exploitation technique

Language: Russian Difficulty level: hard

17:00–18:00

All-in-one REST API: security, tools, and tips

Valentin Mamontov
Application Security Engineer, Swordfish Security

In his talk, Valentin will examine the possibilities of using open-source tools to protect the OpenAPI specification. He will also address its role in API security

Language: Russian

Difficulty level: medium

18:00–18:30

Closing ceremony

Language: Russian

August 23, Friday — Fast track

10:00–10:30

MPoS'tor: attacking the mobile PoS terminal

Georgy Khoruzhenko
Independent security researcher

The speaker will explore an offline payment system based on mobile PoS transactions. He will focus on the opportunities to compromise PoS terminals via the Bluetooth protocol, which in their turn enable the interception of banking card data

Language: Russian

Difficulty level: hard

10:30–11:00

Never give up: move laterally even if you have been blocked in AD

Vladislav Vorobev
SOC L2 analyst, Informzashchita, IZ:SOC

The speaker will explain how the user can move laterally after the account has been disabled in AD and what can be done about it

Language: Russian

Difficulty level: medium

11:00–11:30

One ring to rule the world: analysis of the architecture and security mechanisms of the QRing R02 smart ring

Grigoriy Paguba
Researcher at Institute of Computer Science and Cybersecurity, Peter the Great St. Petersburg Polytechnic University

Grigoriy will talk about his research of QRing R02 and focus on the smart ring's hardware, firmware, and Android app. He will cover the security issues he identified and share his experience of patching the firmware

Language: Russian Difficulty level: easy

11:30–12:00

Researching a multiprotocol USB modem, or Why “S” in IoT still stands for “Security”

Ivan Zorin
Independent researcher

Despite unprecedented security incidents with such "IoT" botnets as Mirai, there are still many devices whose security leaves much to be desired. And with a very particular set of skills and some luck, an unsafe device can be turned into an "attack vector" for other devices. Sometimes it is not at all necessary to have hardcore skills in hardware analysis and reverse engineering.

The talk is intended for a wide range of specialists interested in firmware security. The speaker will review a modern device and explore the use of common software tools for analyzing GNU/Linux-based firmware for embedded hardware

Language: Russian Difficulty level: medium

12:00–12:30

Network fingerprint at the link speed

Ruslan Trifonov
Junior Developer, CyberOK

Automated network fingerprint, ready-to-use solutions to search for products and protocols

Language: Russian Difficulty level: medium

12:30–13:00

One attack at the watering hole to rule them all

Georgii Kumurzhi
Independent researcher

The speaker will offer a fresh look at watering hole attacks. Using examples, he will demonstrate the potential benefits an attacker can gain by injecting malicious JS code into legitimate services of an organization. The icing on the cake will be a detailed breakdown of the cyber kill chain that enables the completion of most pentest and red team projects in just a few steps

Language: Russian Difficulty level: medium

13:00–13:30

LOLApps, the hacker's forage

Kirill Magaskin
Junior Incident Response Specialist, Kaspersky

The speaker will delve into some unusual ways of using legitimate applications in the attacks he investigated recently

Language: Russian Difficulty level: medium

13:30–14:00

Why it is important to create private SAST rules and how to do it correctly

Arthur Sakolchik
Application Security, Positive Technologies

Static code analysis is important for ensuring the security and quality of software. However, using the standard rules offered by most SAST tools is not always enough to identify all possible vulnerabilities and problems specific to a particular project or organization.

Implementing your own rules in a SAST tool is becoming an essential practice that takes into account the unique requirements, architecture, and business logic of your application

Language: Russian Difficulty level: easy

14:00–14:30

Hidden traps in the Apple paradise: unveiling the macOS threats

Irina Kolyagina
Senior Threat Analyst, BI.ZONE

Irina will talk about methods to bypass the built-in security mechanisms and new ways to detect threats in macOS environments

Language: Russian Difficulty level: medium

14:30–15:00

Hacking Bitrix via mobile. How mobile applications help to break through the infrastructure of companies

Aleksandr Larin
Pentester, T.Hunter

How to hack a web application using alternative authentication channels?

Aleksandr will share a personal story of a web application pentest during which his team managed to compromise a whole infrastructure by using the mobile app's vulnerabilities and a bit of OSINT.

He will also give additional examples from his practice to demonstrate how mobile applications directly or indirectly help to compromise the web

Language: Russian Difficulty level: medium

15:00–15:30

IRonBRO, a DIY browser isolation platform to protect against Internet threats

Nickolai Klendar
Independent researcher

Most cyberattacks on organizations employ Internet resources. The categorization engines built into NGFW and Secure Web Proxy solutions are not fast enough. Blocking sites that cannot be categorized or working only with whitelisted ones improves security but impairs employee productivity. End-to-end encryption makes it almost impossible to perform antivirus or data leakage analysis at the NGFW/SWG level even using TLS inspection.

In this talk, Nickolai will review a solution that implements web isolation to protect against Internet threats. This technology enables secure access to Internet resources, excludes the possibility of user interaction with the adversary's C2 system, and prevents the transfer of harmful content to users

Language: Russian   Difficulty level: easy

15:30–16:00

Data infiltration and exfiltration via RDP during a pentest

Denis Dushenev
Deputy Head of the Security Department for Infrastructure Testing, Compliance Control

During a pentest, connection to a remote server can be established via RDP. If the server has a high level of security, the usual methods of copying files to/from the server will not be available. The speaker will explore a data transfer method that involves keyboard input and desktop sharing. He will discuss ways to detect such infiltration/exfiltration methods

Language: Russian   Difficulty level: medium

16:00–16:30

From source maps to secrets

Yegor Borovinskih
Chief Security Specialist, Weblock

Developers are increasingly leaving open source maps in their web applications. Thanks to this, any user can view the source code in its original form. What's wrong with that?

Language: Russian   Difficulty level: medium

16:30–17:00

SBOM into SIEM for incident response and cloud infrastructure security

Alexey Vishnyakov
Senior DevSecOps Engineer, Yandex Cloud

Alexey will explore what essential information should be included in the SBOM and discuss the associated challenges and advantages of sending SBOMs to an SIEM system.

The talk will focus on utilizing CycloneDX tools for SBOM generation and enriching it with essential missing metadata related to builds and artifacts. The presentation will address topics such as File Integrity Monitoring (FIM), identifying vulnerabilities in third-party components (SCA), leveraging SBOMs for efficient incident response, and the obstacles encountered in deploying controlled builds in Yandex Cloud

Language: Russian Difficulty level: medium

17:00–17:30

What to do if you don't know what to do, or Pentesting ISO 8583

Yuri Bichuk
Pentester, Compliance Control

Pavel Popkov
Pentester, Compliance Control

The speakers will share their experience of pentesting an unknown dialect of the ISO 8583 specification

Language: Russian Difficulty level: medium

17:30–18:00

Another incident, or How I ran once more into MikroTik

Vladislav Azersky
Senior DFIR Specialist, F.A.C.C.T.

It is no secret that during attacks, adversaries try to access not just IT administrators' workstations or domain controllers, but also network devices. The speaker will focus on a cybersecurity incident involving MikroTik. He will also discuss several options of testing whether MikroTik network devices have been compromised

Language: Russian Difficulty level: easy

August 23, Friday   Threat.Zone

10:00–10:20

Mind the intelligence gap

Oleg Skulkin
Head of Cyber Threat Intelligence, BI.ZONE

We're always dealing with blind spots. We always see just a part of the whole. We can't solve this problem, but we can do our best to limit it. It's high time to start!

Language: Russian   Difficulty level: easy

10:20–11:10

If money can fix it, it's not a problem: how underground resources help threat actors execute targeted attacks

Daria Sebyakina
Senior Product Marketing Manager, BI.ZONE

In attacks on Russian companies, adversaries often use both custom-made and commercial malware. These programs can be purchased on underground resources as a subscription that includes customer support and regular updates. Often, the developers of such programs explicitly indicate that their solutions may not be used for attacks within Russia. However, this rule has been ignored time and again.

Various underground forums and chats have no shortage of commercial offers from initial access brokers. Assistance in subsequent stages of targeted attacks can be purchased as well.

Does this mean that executing an attack is possible even without possessing advanced technical skills? Daria will explore this in her research of commercial malware employed in targeted attacks on Russian companies.

The speaker will examine the steps threat actors need to take to execute an attack. She will share her view on how one can obtain the necessary tools for that and give examples of commercial malware used in recent attacks

Language: Russian   Difficulty level: easy

11:10–12:00

Nothing cybercriminal

Polina Bochkareva
Cyber Threat Intelligence Analyst, BI.ZONE

Hacktivism has long been a way to get one's point across to the global community. However, since 2022, such attacks have taken on a new form, when the actions of attackers are not condemned or prosecuted, but rather approved and sometimes even supported at the state level. The talk will be devoted to an overview of “hack as a statement” and hacktivism as a phenomenon of the last few years, with respect to Russian and CIS organizations. The speaker will examine the key groups that perpetrated the attacks and will look at their motives, abilities, and methods

Language: Russian   Difficulty level: easy

12:00–12:50

Ransomware for the smallest

Lada Antipova
Head of Response and Digital Forensics Department,
Angara Security

Ransomware is a pain in the neck for everyone: from small businesses to large corporations. While 2022 and 2023 marked the beginning of widespread use of ransomware variants whose source code was leaked online, small and medium-sized businesses (SMBs) were carpet-bombed with little-known strains of ransomware.

Some of those strains vanished into thin air after just a few attacks while others remained active longer. The latter are the subject of Lada's talk. She will delve into the motivation of the adversaries, their actions at the post-exploitation stage, and the measures to take and to avoid while investigating and remediating such attacks

Language: Russian   Difficulty level: easy

12:50–13:40

Sticky case: analyzing the attacks of the Sticky Werewolf group

Dmitriy Kupin
Head of Malware Analysis Team, Threat Intelligence, F.A.C.C.T.

The speaker will examine the Sticky Werewolf cyber espionage group. He will focus on the targets, timeline, tools, infrastructure, TTPs, and attribution

Language: Russian   Difficulty level: medium

13:40–14:30

Hacking MS Exchange is not only about vulnerabilities, or Once upon attack

Alina Sukhanova
Senior Incident Response Specialist, Kaspersky

Alina will share her story of an investigation with a surprise ending. She will address the tactics and techniques used by the attackers, how OSINT helped them gain initial access, and what challenges Alina and her colleagues faced while investigating the case

Language: Russian   Difficulty level: medium

14:30–15:20

Linux endpoint detection: current threats and detection methods

Gago Minosyan
Threat Hunter, Solar 4RAYS

The number of Linux threats is on the rise, so is the need to ensure effective protection of Linux environments. In his talk, Gago will break down the top threats he encountered in real-life investigations and describe the methods to effectively detect such threats

Language: Russian   Difficulty level: medium

15:20–16:10

Journey of winding paths: ExCobalt's maneuvers in attacking Russian companies in 2023-2024

Vladislav Lunin
Senior Threat Intelligence Specialist, Positive Technologies

Alexander Badaev
Threat Intelligence Specialist, Positive Technologies

The presentation will focus on the ExCobalt group and the multiple vectors of its attacks on Russian companies. It will explore the ways in which the group managed to gain initial access: by sending out phishing emails, exploiting the CVE-2023-38831 and CVE-2023-3519 vulnerabilities, and abusing trusted relationships.

The speakers will cover ExCobalt's use of the Facefish rootkit and delve into the group's extensive infrastructure. They will also talk about the new malicious tools, modified standard Linux utilities, and GoRed v0.0.1 they discovered in the open directories of the adversaries.

Finally, the speakers will review all the found versions of GoRed and analyze its links to ExCobalt

Language: Russian

Difficulty level: medium

16:10–17:00

Attacker tools in 2023-2024

Semyon Rogachev
Head of Incident Response Department, Bastion

In his talk, the speaker will analyze the tools that adversaries used in attacks on Linux and Windows environments in Russia. He will also give recommendations on how to detect and analyze such tools

Language: Russian

Difficulty level: medium

17:00–18:00

Panel boozecussion: The state of the Russian threat landscape in 2024

Moderator
Oleg Skulkin
Head of Cyber Threat Intelligence, BI.ZONE

Elena Shamshina
Head of Threat Intelligence, F.A.C.C.T.

Kirill Mitrofanov
Cyber Threat Intelligence Team Lead,
Kaspersky

Igor Zalevskiy
Head of Research Center, Solar 4RAYS

Denis Kuvshinov
Head of Threat Intelligence Department (PT ESC),
Positive Technologies

During the panel, representatives of various cybersecurity companies will discuss this year's changes in the local threat landscape

Language: Russian

August 23, Friday — Community track

10:00–10:20

LockPick: Sesame, open yourself!

ostara
Independent researcher

Zaf0d
Independent researcher

The speakers will delve into the history and culture of lock picking, discuss its relevance to cybersecurity, and offer the audience a chance to solve a small puzzle

Language: Russian   Difficulty level: medium

10:20–11:00

Don't let your keys talk to strangers

Scan87
Pentester

The key and the lock are among the most recognizable symbols of security. A lot has already been said about locks, so this talk will be mainly about keys. We cherish them and are afraid of losing them. But this is far from the only way they can be compromised.

The speaker will talk about key recovery techniques, methods of decoding based on photography, and the process of making functional duplicates. Scan87 will focus on keys to cylinder locks, dimple locks, disk-detainer locks and give a brief overview of RFID card security. He will also share stories of epic fails and the lessons he learned from them

Language: Russian Difficulty level: medium

12:00–13:00

Hundreds, or may be even thousands of bug hunters

Yury Ryadnina
Senior Banking Security Assessment Specialist,
Positive Technologies

Prepare for a joyride full of amusing stories about the Bug Hunter channel and the bug hunting community. Memes, plans, secrets, lifehacks, and a story about the contest Yury organized for the OFFZONE audience. He will make complex things sound simple

Language: Russian Difficulty level: medium

13:00–14:00

Mobile app security: trends and developments of 2024

Yury Shabalin
CEO, Stingray Technologies

The speaker will discuss the most significant news of the mobile security industry and address some latest critical vulnerabilities. He will review the new attack vectors and cool bugs that appeared in mobile applications over the last six months

Language: Russian Difficulty level: medium

14:00–15:00

OSINT as a way of thinking

Dukera
Co-founder, OSINT mindset

The speaker will share his opinion on how OSINT tasks should be solved and explain why the OSINT methodology can be applied to everyday life

Language: Russian Difficulty level: medium

15:00–15:30

Objection! Triage dilemma

Pyotr Uvarov
Head of Bug Bounty, VK

For many people, vulnerability triage is a black box with complex processes and mechanisms. The best way to understand how it functions is to use examples. Pyotr will talk about VK's vulnerability triage process and its challenges. Bug hunters will find it useful to get an insider view of the vendor's processes to build effective communication with triagers

Language: Russian Difficulty level: easy

16:00–16:30

Pentester's tales

Mikhail Driagunov
Pentest Team Lead, Digital Security

Mikhail will share three stories from his experience. The first of them is about spammers making phone calls to people after they just visited a website. The second one deals with the decryption of BitLocker with a logic analyzer. In the third story, Mikhail will talk about how scanning a couple of barcodes on a self-checkout machine in a grocery store resulted in remote code execution

Language: Russian Difficulty level: medium

16:30–17:30

PHP 8+. The backdoor saga

Mark_Tauber
Independent researcher

The release of the eighth version of PHP brought some challenges to the hacking community.

The speaker will discuss the following issues:

- What has changed in PHP and what are the problems?
- Single line server takeover. Is it possible under the new terms?
- It takes an old solution to fix a new problem
- Defense: basic strategies and attack prevention

Language: Russian   Difficulty level: hard

August 23, Friday   AppSec.Zone

10:00–11:00

Defense against transaction time manipulation attack in Hyperledger Fabric blockchain

Igor Agievich
Independent researcher

There is not much publicly available information about the practical security of the Hyperledger Fabric blockchain. However, the framework has been actively used for quite some time in various fields including digital financial assets.

Using the concept of a vulnerable smart contract that imitates a digital financial asset, the speaker will examine the nature of the transaction time manipulation attack and its financial consequences. Igor will present his open-source solution to defend against such an attack. The solution is based on NTP/NTS client and is resistant to man-in-the-middle attack. Hyperledger Fabric smart contract developers can use the solution instead of implementing time manipulation protection on their own

Language: Russian   Difficulty level: hard

11:00–12:00

Cascading AI validation of code defects

Anna Arkhipova
Business Development Manager, IITD Group

Anna will talk about improving the quality of SAST due to AI validation of defects based on graphs correlation of passthrough vulnerability trace.

The speaker will address:

- triage issues
- correlation of defects based on detection of crossing points of pass-through vectors using graph analysis
- approach to the minimum amount of vulnerability metadata in code required for correct defect assessment by AI model
- algorithm for cascading AI defect validation
- effectiveness and advantages of the approach

Language: Russian Difficulty level: hard

12:00–13:00

No more free food! Interesting bugs in e-food apps

Egor Takhtarov
Pentester, CICADA8

This talk examines bugs found in reward programs of e-grocery vendors

Language: Russian Difficulty level: easy

13:00–14:00

How I hacked VK's Neo Capsule

Vladimir Kononovich
Senior Reverse Engineer, BI.ZONE

Vladimir will share his experience of reverse engineering Capsule Neo, a smart IoT device by VK—from holding the gadget for the first time in his hands to writing the final report. The presentation is suitable for all audiences, including those without any knowledge of reverse engineering

Language: Russian Difficulty level: hard

14:00–15:00

Doctor for Docker, or Building a process for managing vulnerabilities in Docker images: from patching to production

Aleksandr Trifanov
AppSec Team Lead, Avito

Aleksandr will talk about the results he and his team were able to achieve in setting up scanning, verification, and patching for Docker images, prioritizing and grouping of vulnerabilities, and the released product fixes

Language: Russian Difficulty level: medium

15:00–16:00

Asset discovery and risk management in product codebase

Dmitrii Mariushkin
Product Security Lead, Ozon Fintech

The speaker will talk about base components of a stereotypical microservice in digital products; what vulnerabilities are associated with these components; how the overall risk is related to the number and structure of objects processed in the service's API, stored in the database, or received in client methods of other services; how to extract the structure of these objects from the code using Semgrep rules and store them for analytics; how to assess the extracted structure and obtain the resulting risk level; and how and where else the discovered data and measured risks can be used

Language: Russian Difficulty level: medium

16:00–17:00

ApiSecurity 101

Alexander Chicailo
Senior Specialist, Application Security Expertise Team,
Positive Technologies

API security is a critical part of modern software. The speaker will analyze various vulnerabilities and attacks aimed at web APIs and ways to address them

Language: Russian Difficulty level: medium

17:00–17:25

EPSS: one more way to prioritize vulnerabilities

Artsem Kadushko
Head of Application Security

Artsem will talk about the exploit prediction scoring system (EPSS), its pros and cons, and whether it has advantages over the tried-and-true methods of vulnerability prioritization

Language: Russian

Difficulty level: medium

17:25–17:50

SCA & SAST: towards the automation of triage

Vitaliy Gulin
Senior Information Security Engineer, Rostelecom

One of the main challenges an application security specialist faces is dealing with alerts from various vulnerability analyzers, the process also known as triage. Vitaly will discuss approaches to this process and review the methodologies tested by his team. He will also share his opinion on the feasibility of using AI to reduce the workload of AppSec specialists

Language: Russian

Difficulty level: easy

17:50–18:00

BUGS ZONE 2.0 award ceremony hosted by BI.ZONE Bug Bounty, VK, T-Bank, CICADA8, MTS, and Kuper

Language: Russian

August 23, Friday — Main track

18:00–18:30

Closing ceremony

Language: Russian