OFFZONE 2023

OFFZONE 2023 SCHEDULE

Full agenda

VIEW MAP

August 24

10:00

Opening ceremony

MAIN TRACK

10:45–11:00 | August 24

Track 1 · Russian · English

11:00

Let's hack old-timers!

MAIN TRACK

Omar Ganiev
Founder, DeteAct

Cybersecurity is derived from technology. Emerging technologies give rise to new threats and new attack vectors.

Such iterative progress tends to go unnoticed. Take a look at the cybersecurity landscape over the past 10 years. Some things have changed drastically, while others have remained strikingly unchanged.

This prompts a question: what should we expect in the next 10 years and should we get prepared for that?

11:00–12:00 | August 24

Track 1 · Russian · English

Throw away your PACS! Wiegand and TM security analysis

dumbmode
Private cybersecurity consultant

Even if you have a modern access control system, it may have vulnerabilities inherited from previous generations. Let's start from 1980

11:30–12:30 | August 24

Community track · Russian

12:00

SPRUSH: what we've learned through 4 years of participation in CTFs

Pavel Blinnikov
Cyber Forensics Specialist, BI.ZONE

The specialist will share his experience as a captain of a strong Russian CTF team

12:00–12:20 | August 24

CTF.Zone · Russian

AntiFraud.Zone opening

Case study

Andrey Ilinskiy
Head of Antifraud Expertise, BI.ZONE

12:00–12:30 | August 24

AntiFraud.Zone · Russian

Deobfuscation and analysis of client-side JavaScript code to detect DOM-based XSS

MAIN TRACK

Andrey Kozlov
Application Security Specialist, Kaspersky

The main purpose of the report is to describe a new automated method for analyzing JavaScript code. Developed by the speaker, the method uses static and dynamic analysis. The expert will compare the results of such analysis with existing automated web vulnerability scanners

12:00–13:00 | August 24

Track 1 · Russian · English

OSS AppSec—coding required (based on a Zen experience)

Andrey Borisov
Cybersecurity Leader, Zen, VK

Andrey will focus on open-source developments in Zen: what problems were encountered and how many things had to be improved on the go. He will also talk about the tools and benefits of the approach drawing on the experiences he gathered with Russia's largest content platform

12:00–13:00 | August 24

AppSec.Zone · Russian

Main cyber fraud trends in the financial industry. Countermeasures

Yury Lysenko
Deputy Chief Information Security Officer, Bank of Russia

Forewarned is forearmed. Attackers are inventing more and more sophisticated scenarios to steal money from people. Thousands of individuals get affected. Some of them lose money they have been saving for years. Knowing how to counteract fraud will help you make the right decision when needed.

The speaker from the Bank of Russia will talk about common fraud schemes and measures taken by the regulator to tackle financial theft

12:30–13:00 | August 24

AntiFraud.Zone · Russian

Paranoid laptop

GreenHamster

Everyone knows what full disk encryption is, but few use it. And if someone thinks about it, they usually postpone it for later because they don't want to reinstall the system and lose its native settings.

The purpose of the report is to remind you that it is possible not to lose anything and to show by example how you can improve the protection of your device with a little effort

12:30–13:00 | August 24

Community track · Russian

Correlation analysis of stream systems

Andrey Sergeev
Senior Specialist, SFB Laboratory LLC

CTF (Capture the Flag) competitions have a category of tasks that require knowledge of cryptography. It takes a solid theoretical background to succeed in solving them. The talk will cover the basics of correlation analysis applicable to stream systems.

The cryptographic community is showing great interest in the development of stream algorithms. For example, various algorithms of the (2G), SNOW (3G), and ZUC (5G) families have been used in mobile communications. Also in 2015, the U.S. National Institute of Standards and Technology (NIST) held a competition in lightweight cryptographic algorithms, which are designed for low-power devices (e.g., IoT). One of the finalists was a stream algorithm called Grain-128AEAD. Such interest in stream systems is attributed to their high-speed characteristics and simplicity of software/hardware implementation.

Analyzing stream algorithms requires special analysis methods. A number of methods proposed in open sources are based on the exploitation of dependencies (correlations) between the characters of the ciphertext and the internal state of the algorithm. Andrey will look into several well-known correlation analysis methods: Siegenthaler's method and the "fast" Meier-Staffelbach method

12:30–13:10 | August 24

CTF.Zone · Russian

13:00

Antifraud. New services in the MIR payment system

Alexey Ipatov
Head of Fraud Monitoring Department, NSPK

The expert will talk about the services deployed in the payment system which are aimed at detecting and preventing fraudulent activity

13:00–13:30 | August 24

AntiFraud.Zone · Russian

NetRunner 2023: Hacker-from-the-future gadgets that can be obtained today

Scan87
Pentester

Yes, cyberpunk has not yet come, but what if you really want to plunge into a futuristic dystopia? In that case, Scan87 offers you a selection of unusual devices and gadgets. He is not sure that they will make life easier, but they will definitely make you feel cool. And will also raise a lot of questions from your colleagues...

13:00–13:30 | August 24

Community track · Russian

5 lifehacks for Mobile DevSecOps

Yury Shabalin
CEO, Stingray Technologies

Everyone knows what the standard web application development process is about and how best to integrate security tools into it. However, few people think about the fact that mobile application development has its own nuances, which can help you significantly improve the effectiveness of security checks.

In his talk, Yury will address these nuances and focus on how to get the most out of security tools, where and what checks can be used, and at what stages they deliver the best outcomes

13:00–13:30 | August 24

AppSec.Zone · Russian

HTTP Request Splitting vulnerabilities exploitation

MAIN TRACK

Sergey Bobrov
Senior Application Security Specialist, Kaspersky

Sergey will talk about HTTP Request Splitting / CRLF Injection vulnerabilities in proxying HTTP requests between web servers. He will look into the methods to detect such vulnerabilities during automated scanning. The expert will also explore their exploitation scenarios on the example of popular bug bounty programs

13:00–14:00 | August 24

Track 1 · Russian · English

Press conference

BI.ZONE Bug Bounty: year-end results

Evgeny Voloshin
Chief Strategy Officer, BI.ZONE

Dmitry Gadar
CISO, Tinkoff

Andrey Levkin
BI.ZONE Bug Bounty Product Owner, BI.ZONE

Ramazan Ramazanov (r0hack)
Bug hunter, Head of External Penetration Testing, DeteAct

Companies are becoming more effective in detecting cyber threats through the combined efforts of in-house cybersecurity specialists and bug hunters. The demand for domestic bug bounty platforms is growing, especially while international platforms are leaving the Russian market.

The press conference will summarize the results of the year as well as highlight the changes in the bug bounty market and how we have adapted to them

13:00–14:30 | August 24

Press.Zone · Russian

Antifraud in 2023: experience and practice of Alfa-Bank

Evgeny Vinokurov
Head of Cyber Fraud Countermeasures Department, Alfa-Bank

In his report, Evgeny will address the following:
- Social engineering involving credit funds
- Simple solutions
- Information exchange problems, current gaps

13:30–14:00 | August 24

AntiFraud.Zone · Russian

Standards-based security for a pentester

Nikolay Umanets
CSO, Rostelecom Contact Center

Nikolay will explain why a pentester needs to know security standards. He will also share how to use this knowledge in building the right attack vector

13:30–14:00 | August 24

Community track · Russian

Purple advanced

Maksim Ilyin
Head of SOC, vulnerability scanner product owner, SolidLab

Igor Landyrev
Security Analysis Specialist, Awillix

The speakers will talk about teamwork in handling incidents and discuss common interaction problems. They will demonstrate a curious case with defender bypassing and share their experience in scaling knowledge gained as a result of testing. They will also come up with a team development concept. You are sure to enjoy it!

13:30–14:00 | August 24

AppSec.Zone · Russian

Exploitation of the debug mode in Chromium, Node, and WebDriver

Denis Pogonin
Senior Application Security Expert, BI.ZONE

The report describes the ways to get RCE when using WebDrivers (ChromeDriver, GeckoDriver) or Node applications in the debug mode. Specifically, it examines the DevTools protocol used to achieve file reading and JS code execution. The report also explores the possibilities of system post-exploitation based on browsers' debug mode

13:30–14:10 | August 24

CTF.Zone · Russian

14:00

Building UBA based on CRM, DLP, and user activity data

Sergey Serov
Head of Antifraud Models Development Team, Tinkoff

The report is devoted to the search for anomalous user behavior in bank systems and the use of ML for these purposes. Sergey will explain how a model for identifying unreasonable actions of employees builds on data from a variety of sources.

Particular attention is paid to the DLP system, which provides events from hosts and triggers of risk rules. By enriching these data with other factors, events are ranked and assessed by severity

14:00–14:30 | August 24

AntiFraud.Zone · Russian

No firmware—be aware. 15 vulnerabilities and other findings in Mitsubishi FX5U PLC

MAIN TRACK

Anton Dorfman
Lead Expert, Reverse Engineering Department, Positive Technologies

The undocumented protocol research algorithm: to get the device firmware, reverse engineer the firmware, send the packets to the device, and check the answers from the device, reconstruct the protocol, find vulnerabilities. What if it's not possible to get the firmware? It seems that only black box analysis or something else might help in this case. "Something else" is exactly what Anton's talk is about.

The speaker will share the approaches to getting information for protocol reconstruction, describe the research results: the protocol structure, the scripts to work with, the 15 CVEs found, and demonstrate PoCs for some of the bugs

14:00–15:00 | August 24

Track 1 · Russian · English

Why aren't all links to be trusted?

Eugene Utkin
Head of Transaction Antifraud Solutions Development, BI.ZONE

Eugene will discuss how to increase trust in the links between settlements to combat social engineering and other takeover scenarios. We will learn what functionality online enrichment should have to combat these fraud scenarios

14:30–15:00 | August 24

AntiFraud.Zone · Russian

Improving GitLab CE security

Savely Krasovsky
Security and Software Engineer, X5 Tech

Many companies use GitLab to manage the software development process. However, in the Community Edition (CE), which is utilized by the majority of these companies, a significant number of security enhancements are unavailable. Over the past year and a half, Savely has managed to bring various premium features into the CE and in some cases even enhanced the existing features within the CE

14:30–15:00 | August 24

AppSec.Zone · Russian

From 0 to 1. About the training for novice members of the CTF world

George Zaitsev
Aka @greg0r0. Ex-Mentor and Methodologist, Olympiad Department for CTF Training, Moscow School of Programmers (MSHP)

The expert will talk about creating a CTF course for absolute novices (who haven't yet solved a single task in their life)

14:30–15:10 | August 24

CTF.Zone · Russian

15:00

How do scam call centers work?

Aleksandr Bolshunov
Leading Expert, PJSC Sberbank

15:00–15:30 | August 24

AntiFraud.Zone · Russian

Conic Finance DeFi protocol hack. How criminals steal millions of dollars without even leaving home

angkasawan
OSINT analyst, Web 3.0 security enthusiast, and private investigator

The report will focus on the essential operation principles of the Conic Finance protocol, the vulnerabilities overlooked by its developers, and the way they were exploited

15:00–15:30 | August 24

Community track · Russian

The weakest chain: a dive into supply chain attacks

MAIN TRACK

Oleg Skulkin
Head of Cyber Threat Intelligence, BI.ZONE

In recent years, supply chain attacks have ceased to be the domain of state-sponsored groups. Our cyber threat intelligence team has unearthed a number of cases where financially motivated perpetrators, including ransomware affiliates, used supply chain attacks to establish initial access to target systems.

In his talk, Oleg Skulkin will explore the inner workings of supply chain attacks. He will use a real case to show at what stage in their life cycle these attacks can be detected to prevent potential damage

15:00–16:00 | August 24

Track 1 · Russian · English

BBusido—the way of the bug hunter

Alexey Lyamkin
Expert, VK

Pyotr Uvarov
Expert, VK

- Bug bounty, an important stage of VK's multilayer security system.
- How VK validates and assesses vulnerabilities.
- How you can grow in bug bounty.
- How VK sees a bug hunter's growth and the severity of identified vulnerabilities.
- Cases and examples of how you can independently test the submitted bugs for the highest possible impact they might have.
- How to disclose vulnerabilities the right way.
- Some interesting bugs discovered on Russian resources

15:00–16:00 | August 24

AppSec.Zone · Russian

COM Objects: Ancient Knowledge

Vladislav Burtsev
Threat Intelligence Analyst, Kaspersky

You will learn the ins and outs of the COM technology and get to know key approaches to researching Windows.
The workshop includes practical assignments to create a COM object, an AMSI Provider, and a client for interaction with system COM servers

15:00–17:00 | August 24

Workshops · Russian

CRC Forge Attack: Operation principle and possible risks

Kirill Komogorov
Penetration Tester, BI.ZONE

The report focuses on the operation principle of the CRC-64 error correcting code and the scope of its application. It also examines a collision attack on this code, including the mathematical foundations. The speaker will demonstrate his own attack automation script as well as the operation of the attack. At the end, he will look into the possible methods to prevent such attacks

15:30–15:50 | August 24

CTF.Zone · Russian

Phantom DLL hollowing aka Module stomping aka Module overloading

Evgeniy Vasilev aka @Not_C_Developer
Pentester, OSEP

Phantom DLL hollowing is a technique for evading antivirus scanners. It enables the attacker to load a legitimate DLL and then inject and execute malicious code

15:30–16:00 | August 24

Community track · Russian

16:00

Buy Now. Pay Later?

Dmitry Rusakov
Fraud Analyst, Yandex

The report delves into some practical issues of fraud prevention in online BNPL services that the speaker had to deal with when building an antifraud solution for a BNPL service

16:00–16:30 | August 24

AntiFraud.Zone · Russian

The current state of the CTF movement and cybersecurity education for high school students in Russia

Daniel Ivankin (@dDanissimo)
Independent researcher

A retrospective field study dedicated to the CTF tendency at Russian schools and its future prospects

16:00–16:30 | August 24

Community track · Russian

A story behind the Codeby CTF platform

Aleksey Morozov
Head of Appsec (Defensive), Tinkoff

Aleksey will speak about his journey from joining a CTF team to launching CTF as a service: how to build your own platform from scratch and turn it into a service (memes included)

16:00–16:40 | August 24

CTF.Zone · Russian

Logical vulnerabilities in Windows local privilege escalation

MAIN TRACK

Vasiliy Kravets
Head of IT Research, Advanced Monitoring

Vasiliy will talk about logical vulnerabilities in Windows apps and focus on respective methods and techniques of their exploitation. He will use real life cases to give advice on avoiding such vulnerabilities in software development. The speaker will also share his experience of communicating with the vendors whose products contained vulnerabilities

16:00–17:00 | August 24

Track 1 · Russian · English

Information security business partners: expectations vs reality

Georgiy Rudenko
Business Information Security Officer, Raiffeisen Bank

Aleksey Guskov
Senior Information Security Business Partner, Raiffeisen Bank

Alexey and Georgiy will talk about their experience with the implementation of the Information Security Business Partner role:
- background and expectations for the role
- IS BP framework (full operating life cycle)
- main "pitfalls" in the IS BP implementation
- examples and challenges of BP operations
- plans for development

16:00–17:00 | August 24

AppSec.Zone · Russian

Reducing the attack surface for the GitLab CI environment

n0nvme
Independent researcher

The speaker will explain how to assemble container images without accessing the Docker socket

16:30–16:45 | August 24

Community track · Russian

Antifraud evolution

Nikolai Dosh
Product Development Manager, Fuzzy Logic Labs

Over the past few years, there has been a significant shift in the payment infrastructure in terms of vectors and technologies of fraudulent attacks. In particular, bank customers are actively attacked through social engineering, which has become one of the world's most widespread types of fraud. However, this was not always like that.

The report will look into the evolution of fraudulent schemes and antifraud technologies. Today, such technologies rely on international data and latest information about attacks on ATMs. The report will also explore fraudulent schemes employing social engineering methods, with examples of incidents in Russia and abroad

16:30–17:00 | August 24

AntiFraud.Zone · Russian

How ads track you

Andrey Kosorukov (dot)
Independent researcher

Andrey will talk about the past, present, and future of online ad targeting and more

16:45–17:00 | August 24

Community track · Russian

17:00

A guideline on keeping your cool when things go to hell

cringineer kringuxovich
Independent (non)security ranter

A collection of peaceful real-life engineering cases where the unintended presence of cybersec created a DRAMA (and usually quite a bizarre one; and not always created, but rather highlighted an already existing one). In a nutshell, a bunch of work related stories for shits and giggles :)

17:00–17:15 | August 24

Community track · Russian

Unusual cyberattacks utilizing well-known remote access tools

Alina Sukhanova
Independent cybersecurity researcher

Has it ever occurred to you that your remote access tools can be used by somebody else? The expert will talk about attacks against small and medium businesses and the ability to launch such attacks as a result of poor security practices when using a well-known remote access tool

17:00–17:30 | August 24

AntiFraud.Zone · Russian

YATB: how to create a fast and lightweight checksystem

Dmitry Zotov
Captain of the kks CTF team

Dmitry will share how his team made another checksystem for a jeopardy CTF: what it is for, what problems the team encountered, and how they are going to develop the system in the future

17:00–17:40 | August 24

CTF.Zone · Russian

Modern reverse engineering automation in HexRays decompiler

MAIN TRACK

Semyon Sokolov
Specialist, Positive Technologies

In his report, Semyon will explore current reverse engineering automation tools and will also present the new ones

17:00–18:00 | August 24

Track 1 · Russian · English

Secure OSS—push and suffer!

Konstantin Kryuchkov
Open-Source Security Expert, Swordfish Security

Software development using third-party components is the one key to save your time to market, but just before you start checking them for security and compliance.

Konstantin will explore the reasons why 3PL security analysis is still about pain and suffering and the ways to make it more comfortable for security and development teams. He will speak about the current issues, approaches, taxonomies, vulnerability databases, and OSS protection methods

17:00–18:00 | August 24

AppSec.Zone · Russian

Symbolic execution of TON smart contracts

@hacker_volodya
Independent researcher

@hacker_volodya will show a prototype of his symbolic execution framework for TON smart contracts (based on Z3 SMT solver). He will talk about the problems he encountered along the way and explain why his framework differs from similar ones for EVM-based blockchains.

He will also demonstrate the framework in action using some simple smart contracts as examples: how to find vulnerabilities and prove preset statements in such contracts

17:15–17:30 | August 24

Community track · Russian

A reverse look at reverse engineering

Boris Ryutin
Security researcher

Reverse engineering is a process of analyzing the code of a research object to understand how it works. The process can be used to analyze security, improve performance, and create new functionality. Or can it? Boris suggests discussing it together

17:30–17:45 | August 24

Community track · Russian

Between a scammer and a money mule

Dmitry Dudkov
Antifraud Pre-Sales Manager, F.A.C.C.T.

What cybercriminals have succeeded in, why you should pay close attention to money mules, and how to counter it all

17:30–18:00 | August 24

AntiFraud.Zone · Russian

Flagging it right: is ML the way to go?

Artyom Menisov
AI and cybersecurity researcher

The workshop will focus on the sensitivity of cybersecurity tools and the importance of prompt response to computer incidents. You will look into a number of cases, including robust solutions

17:30–19:30 | August 24

Workshops · Russian

Voltage glitching for dummies

Egor Koleda (radioegor146)
Independent security researcher

A personal account about dealing with voltage glitching

17:45–18:00 | August 24

Community track · Russian

18:00

Reverse engineering of ~~Python~~ C binaries

Pavel Blinnikov
Cyber Forensics Specialist, BI.ZONE

This talk is about the analysis of some weird binary that Pavel got during incident response

18:00–18:15 | August 24

Community track · Russian

Bosintus

Alexandr Goncharov
Penetration Tester, Innostage

The expert will talk about OSINT in CTF, examine the main tools that are most often used in the tasks, and analyze a lot of real-life examples

18:00–18:40 | August 24

CTF.Zone · Russian

MikroTik Nightmare

MAIN TRACK

Caster
Network security expert

The author's research into MikroTik hardware security in the offensive genre. It covers RouterOS security flaws, pivoting techniques, post-exploitation, MitM attacks, traffic hijacking, as well as a special remix of s0i37 operation, where the expert found a new way of L2 tunneling against Windows machines using a MikroTik route

18:00–19:00 | August 24

Track 1 · Russian · English

August 25

10:00

Breaking the CI/CD

Pavel Sorokin
Lead Security Engineer, Ozon

The workshop will guide you into the security of CI/CD components and pipelines, the hacking of which is often overlooked in standard pentests

10:00–12:00 | August 25

Workshops · Russian

LockPick: how do they do it?

ostara
Independent information security researcher

Zafod Beeblebrox
Independent information security researcher

As always, ostara and Zafod Beeblebrox will share and demonstrate how the locks were supposed to be picked. A look into the booth quests, a bit about the preparations, and the much anticipated gifs!

10:30–11:00 | August 25

Community track · Russian

11:00

Forgot the combination again? How combination locks work

Scan87
Pentester

They are trusted with everything: from luggage in a suitcase to bicycles. From yard gates to safes. But is this trust justified? In the report, the speaker will talk about the workings of combination locks, explore the principle of operation, and, of course, discuss vulnerabilities! In the end, he will try to answer the question, "Is it possible to crack the code to the safe, as spies do in movies?"

11:00–11:30 | August 25

Community track · Russian

Vulnerabilities in AI-generated code

Maxim Karasev
C System Software Developer

Regardless of their imperfections, neural networks are becoming ever more popular among programmers. The speakers will look at the reasons why the networks can generate erroneous code, how severe these errors can be, and what developers can do to minimize risks

11:00–11:30 | August 25

Track 2 · Russian

How to fuzz thousands of applications: A practical guide

MAIN TRACK

Roman Lebed
Cybersecurity Architect, Tinkoff

The talk is aimed at listeners who are familiar with fuzzing technology and those who wish to integrate it into their own SDLC.

Roman will share his personal experience of fuzzing enterprise applications, both on the offensive side (red team) and on the defensive side (AppSec, DevSecOps). Despite the same technology, tools, and goals (vulnerability detection), success requires completely different approaches from each side—despite the presence of thousands of fuzzers running, we are still seeing vulnerabilities in the most popular browsers.

Also, the talk will cover the problems of existing approaches and tools, the complexity of their application for fuzzing thousands of corporate microservices. You will learn how a platform approach to development allows you to offer a flexible and scalable application fuzzing service, transfer unique expertise to the code, and delegate the implementation of fuzzing tests to the product development team.

In other topics, Roman will discuss how you can prioritize targets for fuzzing, based on automated attack surface analysis and data-driven approaches. As a bonus, a couple of examples of vulnerability detection in applications with memory-safe languages

11:00–12:00 | August 25

Track 1 · Russian · English

Bug hunting: cases, tools, and recommendations

Ramazan Ramazanov (r0hack)
Bug hunter, Head of External Penetration Testing, DeteAct

- Why can't you find vulnerabilities for bug bounty?
- Bug hunting methods and cases for each method.
- Russian bug hunting: what is it all about?

11:00–12:00 | August 25

AppSec.Zone · Russian

Symbolic SAST from open-source components

Andrew Pogrebnoi
Junior Specialist, CyberOK

There are quite a few open-source SAST solutions, but as a rule, they are limited to one analysis technique, for example, pattern-matching by code or AST. More complex techniques, such as symbolic execution, are mostly found in commercial solutions. The report will demonstrate how to assemble a SAST pipeline that implements relevant analysis techniques from open-source components, and the results of testing on real applications

11:30–12:00 | August 25

Track 2 · Russian

Solutions to day 1 booth tasks

n0nvme
Independent researcher

The report will explore the quest tasks offered to the participants on the first day of the conference and the possible ways to solve them

11:30–12:30 | August 25

Community track · Russian

12:00

CTF as an expert's Swiss knife

Dmitry Pinin
Deputy Head of Innovative Technologies and Cybersecurity Department, AP Security

The report focuses on CTF as a multifaceted tool for the development of a future information security specialist. Dmitry will share how students are developing the movement in the face of various difficulties, what else hides behind the phrase "played CTF," and will give an example of how to search for problems that beginners might have

12:00–12:20 | August 25

CTF.Zone · Russian

When computers were adults: z/OS penetration testing workflow

Denis Stepanov
Senior Penetration Testing Specialist, Kaspersky

Alex Korotin
Senior Specialist for the Security Assessment Center, Kaspersky

The talk will focus on the penetration testing workflow for z/OS-based systems

12:00–12:30 | August 25

Track 2 · Russian

Passwordless authentication. How WebAuthn can protect your application

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

The report focuses on what WebAuthn is and how this technology protects against attacks and vulnerabilities associated with authentication. Alexander will show the evolution of authentication methods over the last century and the existing methods of passwordless authentication

12:00–12:30 | August 25

AppSec.Zone · Russian

A variety of fuzz farms and why you'd need one

MAIN TRACK

Boris Ryutin
Security researcher

Pavel Knyazev
Reverse engineer, security researcher

Fuzz testing is becoming increasingly popular, and the multitude of relevant tools is ever expanding. A fuzz farm is one of such tools. It provides some orchestration over a set of fuzz engines that help to organize either continuous or interrupted fuzz testing. Initially, such farms are most often just a set of several scripts, which can evolve to something colossal as the need arises.

In their talk, Pavel and Boris will focus on some of the popular solutions and go through what it takes to create a unique fuzz farm

12:00–13:00 | August 25

Track 1 · Russian · English

Insecurity of restaurant pager systems

Anton Ostrokonskiy
Head of Penetration Testing Department, Deiteriy Lab

Restaurant pagers are becoming increasingly popular in cafes and food courts. However, the technologies behind these appliances are completely unsafe.

Anton will explain how these pagers work and cover the types of these devices currently available on the market along with their functionality. He will use several popular models to demonstrate their vulnerabilities and discuss the potential impact that may stem from them

12:30–13:00 | August 25

Track 2 · Russian

Avito's Code Security Platform: a scalable shift-left system one cannot build with DefectDojo

Nikolai Khechumov
Staff Security Engineer, Avito

The report dives deep into Avito's flexible, highly automated scan orchestration and vulnerability management system: event-based at its core, where every finding has its history, state, and lots of valuable metrics

12:30–13:30 | August 25

AppSec.Zone · Russian

OSINT as a way of thinking

Dukera
COO, OSINT mindset community

The expert will talk about his approach to dealing with OSINT quests and show how the OSINT methodology can be applied outside the professional domain—in the everyday life

12:30–13:30 | August 25

Community track · Russian

Pentesting Android mobile applications

Igor Krivonos
Android developer (Java/Kotlin), penetration testing specialist (Android/iOS), security engineer, Python developer, lecturer of mobile device security and Android development in Python

During the workshop, you are going to pentest a quasi-real Android application and learn more about the different aspects of finding bugs and vulnerabilities

12:30–14:30 | August 25

Workshops · Russian

Devirtualization of obfuscated executables

Ilya Titov
Principal Reverse Engineer, CTF SPRUSH team

The talk will explore the workings of the control flow virtual machine obfuscation as well as the possible ways to simplify the analysis of such programs. Join the discussion on initial analysis, converting bytecode to mnemonic form, and decompiling virtual machine bytecode.

All that you need is confident C/Python programming skills, basic skills with IDA/Ghidra reverse engineering environments, the ability to read and understand assembly code and decompile its simplest cases in your head.

Your device should have 5–10 Gb of free space on the hard drive and an x86_64 IDA Pro processor architecture with an x86/x64 decompiler.

We'll give you an assignment, presentation slides, modules for developing Ghidra plugins and an IDE to work with them

12:30–15:30 | August 25

CTF.Zone · Russian

13:00

EAP-Mirror: WPA2-Enterprise and 802.1x Attack

Pavel Yakovlev
Junior Penetration Testing Specialist, Kaspersky

Alexander Volkov
Junior Penetration Testing Specialist, Kaspersky

Wi-Fi pentests have been losing popularity in recent years. Breaking through a corporate Wi-Fi point does not necessarily get you to the internal network. The most attractive Wi-Fi access points most often work only via EAP-TLS.

The EAP-TLS protocol is considered the most secure authentication solution for enterprise networks. The main reason for this: the use of PKI to authorize the client and server

13:00–13:30 | August 25

Track 2 · Russian

CASR: your life vest in a sea of crashes

MAIN TRACK

Andrey Fedotov
R&D Team Lead, Ivannikov Institute for System Programming of the Russian Academy of Sciences (ISP RAS)

Alexey Vishnyakov
Senior DevSecOps Engineer, Yandex Cloud

CASR is an open-source crash triage framework designed to handle post-fuzzing challenges in security research and software development. It enables crash report generation, deduplication, clustering, and severity estimation while being integrated with modern fuzzers like AFL++, LibAFL, and libFuzzer.

CASR supports multiple architectures (x86, ARM, RISC-V), programming languages (C/C++/Go/Rust/Python/Java) and includes LibCASR for the development of custom analysis tools. It also offers casr-dojo for exporting crashes to DefectDojo. CASR is a valuable tool for security researchers and developers dealing with fuzzing and vulnerability management.

The CASR tool set implements the following fuzzing crash triage pipeline: crash report creation with all necessary information for manual analysis, significant reduction of duplicate crashes, clustering, creating UBSAN reports, and uploading new reports to the DefectDojo vulnerability management system

13:00–14:00 | August 25

Track 1 · Russian · English

AnyDOOM: Anycast M4 Plus device security research

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

The report is divided into two parts.

In the first part, Grigoriy will talk about the conducted studies on the security of the Miracast receiver Anycast M4 Plus.

In the second part, he will show you how to run the DOOM game on this device using the knowledge about the device, gained through research from part one

13:30–14:00 | August 25

Track 2 · Russian

Simply interesting. Engineering aspects of software analysis in the FSTEK of Russia paradigm

Dmitry Ponomaryov
Deputy CEO and Director of SSDL Department, Fobos-NT Scientific and Technical Center; Specialist, Ivannikov Institute for System Programming of the Russian Academy of Sciences; Lecturer, Bauman Moscow State Technical University

Dmitry will speak about the development vector of the FSTEK of Russia regulatory framework with regard to certain engineering practices. He will also focus on the centers of excellence specialized in Linux kernel and critical component security analysis under the FSTEK of Russia and Ivannikov Institute for System Programming of the Russian Academy of Sciences. Finally, he will talk about the center of excellence engineering community and its information resources

13:30–14:00 | August 25

AppSec.Zone · Russian

Oops! We did it again, and how to deal with that

}{отт@бь)ч
Engineer, Arh29IT (ex DC78182)

PseudoUnicorn
IT Specialist, Arh29IT (ex DC78182)

The problem of data loss and recovery is becoming less acute with every passing year, but never seems to go off the agenda.

The speakers will explain what to do if you happen to become the lucky one who falls within one percent. They will also present an algorithm of actions at their booth

13:30–14:30 | August 25

Community track · Russian

14:00

Serverless security

Igor Grebenets
AppSec Expert, MTS RED

The talk will cover the security of serverless applications and some of the features related to this topic

14:00–14:30 | August 25

Track 2 · Russian

Kubernetes pentest all-in-one: the ultimate toolkit

Sergey Kanibor
R&D / Container Security, Luntry

When you are pentesting or auditing a Kubernetes cluster, you certainly use automated tools to perform the checks. But what if your cluster is network-limited and you can't download the tools you need inside the Pod? Or it's a readonly container file system? In this case, the only solution is to use a prepared image, inside of which there are all the tools you need.

In his research, Sergey will talk about an image that includes all possible popular tools for pentesting a Kubernetes cluster, including those with automatic checks. He will also present his open-source version complemented with various features, for example, bypassing detection by means of signature engines

14:00–15:00 | August 25

AppSec.Zone · Russian

Fuzzing for SDL: select, cover, reveal

MAIN TRACK

Alexey Vishnyakov
Senior DevSecOps Engineer, Yandex Cloud

Vartan Padaryan
Head of Binary Code Reverse Engineering Laboratory, Ivannikov Institute for System Programming of the Russian Academy of Sciences (ISP RAS)

Vladislav Stepanov
Engineer, Ivannikov Institute for System Programming of the Russian Academy of Sciences (ISP RAS)

Fuzz testing is one of the basic techniques used in secure software development. To reap its benefits, developers must deeply integrate fuzz testing into software development processes and establish links with attack surface analysis, functional testing, sanitizers, automated parsing of detected failures.

The talk covers both the fuzz engine and the process of selecting fuzz targets. Dynamic taint analysis coupled with virtual machine introspection allows you to find interfaces of complex software, through which an intruder will attack your software in the first place, and prioritize the fuzz order in resource-constrained environments. And hybrid fuzz testing with dynamic symbolic execution helps you quickly achieve good code coverage and detect errors even if they do not immediately lead to visible software failures

14:00–15:00 | August 25

Track 1 · Russian · English

Testing gRPC web applications via Burp Suite

Ilya Danenkov
Pentester, Deiteriy Lab

Ilya will talk about performing gRPC security testing of web applications with Burp Suite. This tool does not have built-in capabilities for protobuf deserialization. The available extensions for Burp Suite are not widely used and have only limited functionality for gRPC testing.

With this talk, Ilya wants to raise awareness about gRPC testing and present his own extension for gRPC research

14:30–15:00 | August 25

Track 2 · Russian

Flipper Zero usage in Red Team projects

Georgii Kumurzhi
Chief Engineer of the Cybersecurity Department, PJSC Sberbank

The report describes practical cases of using Flipper Zero when modeling an external intruder, examines custom settings and firmware, as well as the options for masking this device

14:30–15:00 | August 25

Community track · Russian

15:00

A fairy tale about external components

Aleksandr Trifanov
Lead Engineer, Avito

The report introduces Avito process for external components management. It covers problems and solutions for early detection, blocking, and auto-fixing vulnerable dependencies

15:00–15:30 | August 25

AppSec.Zone · Russian

Nuclei: Expanding the Possibilities of Modern Pentest Methods

Alexey Vistorobsky
Pentester, Awillix

When testing for penetration, very often many tools are undeservedly ignored, despite the fact that they have great potential, both in the field of testing and its automation. The report will focus on the Nuclei tool and its role in pentesting. Examples of searching for specific CVEs, analysis of ready-made templates and examples of integrating Nuclei with other tools from the point of view of both business and pentests

15:00–15:30 | August 25

Track 2 · Russian

Vulnerabilities in Bitrix24. CVE-2022-43959

Dmitrii Lymbin
Head of Software Security Research, SecWare, DC78412

Sergey Avdeev
Software Security Researcher, SecWare, DC78412

The specialists will explain how Bitrix24 vulnerabilities can make it easier for hackers to take over an organization's domain controller.

They will focus on how CVE-2022-43959 was found, why this vulnerability occurs, and how the developers fixed it. Dmitrii and Sergey will also demonstrate kill chain attacks and share how they reported this vulnerability

15:00–16:00 | August 25

Community track · Russian

Wire is good, wire is reliable: security research of WirenBoard subsystem

MAIN TRACK

Alexey Usanov
Head of HW_LAB, Positive Technologies

This research explains some security issues in the WrenBoard subsystem. Alexey will share how to produce an MitM attack between the central unit and remote controlled sensors.

He will talk about sensors hardware and how this research proceeded to another research on GigaDevice microcontrollers with a lot of security issues being found. By using those vulnerabilities, it was possible to decrypt sensor firmware updates, gain access to some sensitive data, and implement RCE

15:00–16:00 | August 25

Track 1 · Russian · English

Pivoting

Yaroslav Shmelyov
CyberED Lecturer, Standoff 2022 prize winner (as a member of the Invuls team)

The workshop will delve into the tools used in traffic tunneling and the basics of their operation. In particular, it will examine some of the tunneling options for different operating systems. Other topics include ports forwarding, traffic obfuscation, and masquerading as legitimate protocols. You are going to be working on virtual machines

15:00–17:00 | August 25

Workshops · Russian

A couple of words about HQL injections

Denis Derevtsov
Pentester, Deiteriy Lab

Currently, Hibernate Query Language (HQL) injections continue to pose a significant threat to applications that use Hibernate or similar ORM frameworks.

During this session, the speaker will talk about common attack vectors, prevention techniques, and potential consequences of successful HQL injections exploitation.

In addition, the speaker will demonstrate several real-world cases where HQL injections were exploited

15:30–16:00 | August 25

Track 2 · Russian

Pentest of LLM in client applications

Artyom Semenov
Penetration Tester, RTM Group

Language models are starting to make their way into client applications. We see banks and other organizations employ them to communicate with users and process information. Attackers are aware of that and adjust their ploys accordingly.

One example is the case of the MathGPT attack, where an attacker was able to make an LLM execute code on the server.

In his talk, Artyom will present a methodology for pentesting such applications and elaborate on the associated risks and his findings. He will also share some testing tools

15:30–16:30 | August 25

AppSec.Zone · Russian

Asymmetric elliptic curve cryptography

Alexander Sokolov
Cryptographer, SPRUSH CTF team

You will get acquainted with the tools to work with elliptic curves, some of the protocols, and possible vulnerabilities in these protocols.

The workshop will guide you into the structure of elliptic curves and their applications in the modern world. You will understand the importance of selecting curve parameters and will examine some cryptographic schemes using ECC: ECDH, ECDSA.

You should have familiarity with Python syntax and ideally possess basic knowledge of algebraic groups.

Your machine should have Python libraries: PyCryptodome, fastecdsa, py-ecc. Make sure to install CryptoHack Docker Container and, optionally, SageMath (present in CryptoHack).

You will be provided with presentation slides and interactive step-by-step instructions for practical tasks

15:30–18:00 | August 25

CTF.Zone · Russian

16:00

Evalsploit: one-line server takeover

Mark_Tauber
Independent researcher

Mark_Tauber's report deals with one-line backdoors in an environment of restricted server functions and permissions.

The speaker will cover the following topics:

- WAF evasion: how to avoid falling victim to it?
- Why was this topic abandoned, what potential does it hold, and what were we able to achieve in a restrictive environment?
- How to defend from such threats?

16:00–16:30 | August 25

Community track · Russian

Trade-off: free movies for credentials, a Linux supply chain attack story

Leonid Bezvershenko
Security Researcher, Kaspersky

Georgy Kucherin
Security Researcher, Kaspersky

While investigating a security incident, the experts discovered that a popular download manager for Linux was doing something the user would never expect. Attend the talk to find out the whole story!

16:00–16:30 | August 25

Track 2 · Russian

GigaVulnerability: GD32 Security Protection bypass

MAIN TRACK

Alexey Kovrizhnykh
Security Researcher, Positive Technologies

When developing hardware solutions based on microcontrollers, manufacturers want to protect their firmware from falling into the wrong hands. To do this, most microcontrollers implement readout protection technologies. Do they protect well?

The first part of the talk will briefly describe the existing attacks on these technologies. The second part will be devoted to our research on the security protection technology of GD32 microcontrollers (GigaDevice) and the vulnerabilities found that allow obtaining the contents of the memory despite the protection enabled

16:00–17:00 | August 25

Track 1 · Russian · English

How we generated SBOM and what came out of it

Artsem Kadushko
Application Security Lead

In his talk, Artsem will discuss the path he has traveled in creating his software composition analysis process, namely, the generation of the SBOM file. In addition, he will explain why one tool cannot solve all the problems in SBOM generation

16:30–17:00 | August 25

AppSec.Zone · Russian

Hide if you can: Extending WinRM Detection Opportunities

Anton Velichko
Head of Digital Forensics and Malware Analysis Lab, F.A.C.C.T.

It's no secret that attackers quite often use the Windows Remote Management service to move around the infrastructure. In his talk, Anton will consider what artifacts will indicate the use of WinRM.

He will also talk about an undocumented artifact of this service and how to use it to quickly identify hosts being exploited by attackers, including when event logs have been deleted

16:30–17:00 | August 25

Track 2 · Russian

It's web again, it's servers again, and it's all in **** again

Roman Ananev
DC78422

Let's talk about the web again, let's talk about servers again, let's talk about infrastructures and how leaky they are. And yes, despite the fact that new and newer technologies with old problems are being introduced again and again, they are not the problem %)

16:30–17:00 | August 25

Community track · Russian

17:00

SOC processes you can't find in books

Sergey Soldatov
Head of SOC, Kaspersky

Improvements are the result of an efficient analysis of own mistakes. In a 15-minute talk, Sergey will speak about such mistakes and the processes implemented in his SOC to prevent such mistakes.

The talk can be useful for SOC managers and methodologists as well as those who provide related consulting services

17:00–17:30 | August 25

Track 2 · Russian

How to hide your actions when every step is being monitored

MAIN TRACK

Ivan Gavrilov
AppSec Engineer, Innostage

Modern security tools are increasingly relying on eBPF technology to monitor events on hosts. Its capabilities seem to enable security teams to see everything and prevent the slightest compromise attempt in a timely manner. Or not?

In his report, Ivan will consider the strengths and weaknesses of the eBPF technology for security tasks as well as the possible methods to hide your actions using the example of existing eBPF-based security tools

17:00–18:00 | August 25

Track 1 · Russian · English

Bugs on the Orbit

Tatiana Kurmasheva
Independent expert

Nowadays, the creation and launch of small spacecraft is becoming more and more affordable. There are already about 5,000 active satellites in the Earth's orbit.

Tatiana will take a look at the current state of things from the information security perspective. Along the way, she will explore the features of the protocols and the configuration of modern small spacecraft

17:00–18:00 | August 25

Community track · Russian

Malware and cryptography

Zhassulan Zhussupov aka @cocomelonc
Malware Analyst, MSSP Global

The report is dedicated to the role of cryptography in the development of malware and to payload encryption using classic cryptographic algorithms.

Zhassulan will delve into the practical research on using TEA, Madryga, RC5, A5/1, Z85, DES, and other encryption algorithms and share its outcomes. Also being investigated is the applicability of cryptography based on elliptic curves. The attendees will learn how this influences the VirusTotal detection score, and how it can be applied to bypassing antivirus software

17:30–18:00 | August 25

Track 2 · Russian

18:00

Closing ceremony

MAIN TRACK

18:15–18:30 | August 25

Track 1 · Russian · English