BSides Berlin Security Training: Full-Day Practical Workshop on IT and AI Security

"A Phishing Trip with the Bears" – Hands-on Malware Analysis and Phishing Defense Training

Date: Thursday, 12 November 2026, 09:00–16:00 (a standalone training day, the day before the BSides Berlin conference) · **Venue:** CIC Berlin, Lohmühlenstraße 65, 12435 Berlin, private seminar room · **Application reference number:** 135944 · **Recognized** under the Berlin Education Leave Act (Bildungszeitgesetz), Bescheid II A 75 - 135944

TIME	UNIT	CONTENT	FORMAT
08:30–09:00	–	*Registration and attendance check-in*	–
09:00–09:45	1	Introduction: workshop flow and quiz platform; background on APT28 ("Fancy Bear") and the geopolitical context of phishing campaigns	Talk + short practical quiz
09:45–10:30	2	Payload delivery and exploitation: analyzing a real phishing email, indicators in mail headers, dissecting a malicious MS Office attachment with open-source tools	Short lecture + hands-on exercise, quiz review
10:30–10:45	–	***Break***	–
10:45–11:30	3	Installation, command and control, persistence: Windows persistence techniques, steganography, simple cryptography and deobfuscation, .NET malware analysis, abuse of cloud services	Short lecture + hands-on exercise, quiz review
11:30–12:15	4	Phishing backend investigation I: open directories in attacker infrastructure, anatomy of the Roundcube campaign, web attack vectors	Talk + short practical quiz
12:15–13:15	–	***Lunch break***	–
13:15–14:00	5	Phishing backend investigation II: safely analyzing credential phishing websites, investigating Cross-Site-Scripting vectors	Hands-on exercise validated via the quiz platform
14:00–14:45	6	APT29 PDF attack chain I: analyzing a malicious PDF file and local malicious JavaScript (guided)	Guided hands-on exercise, solo or in pairs
14:45–15:00	–	***Break***	–
15:00–15:45	7	APT29 PDF attack chain II: independent analysis of the multi-stage sample with trainer support; recap, transfer to your daily work, final quiz	Hands-on exercise + moderated wrap-up
15:45–16:00	–	*Closing, handout of participation certificates*	–

1. Learning objectives

By the end of the training, participants will be able to (1) systematically analyze phishing emails and extract indicators from mail headers and malicious Office and PDF documents, (2) trace, investigate and document multi-stage malware attack chains from real threat actor groups (APT28 "Fancy Bear", APT29 "Cozy Bear"), and (3) safely identify and assess attacker infrastructure (phishing backends, open directories, web attack vectors such as Cross-Site-Scripting). These skills apply directly to day-to-day work in security analysis, incident response and secure software development.

2. Target audience

Cybersecurity professionals and IT-related students, as well as IT staff whose work touches on security aspects (e.g. software development, system administration, cloud/DevOps, AI security). The workshop is deliberately paced for beginners; no prior malware analysis experience is required, basic familiarity with the Windows operating system is a plus.

3. Content (three sequential parts)

Part 1 – APT28 phishing attack chain (3 units): analysis of a real phishing campaign, from the email through malicious Office attachments to persistence, command-and-control, steganography, simple cryptography and deobfuscation, and .NET malware analysis; how attackers abuse open-source tools and cloud services.

Part 2 – Investigating a phishing backend (2 units): identifying open directories in attacker infrastructure, safely analyzing credential phishing websites (Roundcube campaign), investigating Cross-Site-Scripting attack vectors.

Part 3 – APT29 PDF attack chain (2 units): applying the techniques from parts 1 and 2 to a real, multi-stage malicious PDF; analyzing malicious PDF files and local malicious JavaScript; wrap-up and transfer to your own daily work.

4. Didactic and methodological concept

A continuous mix of short theory inputs (max. 45 min. each) and guided hands-on exercises on your own machine. An interactive quiz platform with real-time results accompanies every unit: the instructor can see each participant's progress as it happens and give targeted guidance (continuous learning-objective tracking). Exercise material, slides and working environments are all provided; no installation is required on participants' own devices. Individual and paired work during the exercises encourages interaction between participants.

Group size: max. 30 participants, fixed group for the whole day (named tickets, separate "Security Training Track" ticket category; no switching between the training and other program parts). The quiz platform and supervised exercise phases ensure a sufficient level of interaction throughout.

Course lead: Natalie Mahlow, planning and running technical training formats professionally since 2018; known to participants by name and present for the whole day.

Instructor: Marius Genheimer, DFIR Specialist and Threat Researcher, SECUINFRA Falcon Team (Berlin); instructor for the five-day OSDA defensive training (Red&Blue Alliance); 2026 workshop engagements include BSides Ljubljana, BSides Luxembourg, BSides Vilnius and Pass the SALT.

5. Organizational details

- **Attendance tracking** throughout the day: sign-in sheet at registration and after the lunch break, checked against the named participant list by the course lead.
- **Participation certificate:** free of charge, stating title, date, scope (7 units of 45 min.), content and the course lead's signature.
- **Fee:** 179 EUR (early bird) / 239 EUR, including materials and certificate.
- **Accessibility:** step-free access, accessible restrooms; individual needs are asked for at registration; all materials available digitally in screen-reader-friendly format in advance; assistants attend free of charge.