POSITIVE HACK DAYS

ORGANIZER

POSITIVE TECHNOLOGIES

Program

Tech

Hands-on Labs

Fast Track

Backslash powered scanning: implementing human intuition

Author: James Kettle

Want to visit +16 Tech

Existing web scanners search for server-side injection vulnerabilities by throwing a canned list of technology-specific payloads at a target and looking for signatures—almost like an anti-virus. The speaker will share with you key insights from the conception and development of an open-source scanner evolved from classic manual techniques that's capable of finding and confirming both known and unknown classes of injection vulnerabilities.

- Language
- English

Head of Research at PortSwigger Web Security, where he designs and refines vulnerability detection techniques for Burp Suite's scanner. Recent work has focused on techniques to detect unknown classes of vulnerabilities and exploiting subtle CORS misconfigurations in bitcoin exchanges. He has extensive experience cultivating novel attack techniques, including server and client side RCE, and abusing the HTTP Host header to poison password reset emails and server side caches. He has previously presented at numerous prestigious conferences, including BlackHat and AppSec.


James Kettle

Do WAFs dream of statistical analyzers

Author: Vladimir Kochetkov

Want to visit +15 Tech

Head of the application security assessment team at Positive Technologies. He is engaged in the development of PT Application Inspector being an expert in application security and applied cryptography. He participated in such projects as Nemerle, YAPOET, and SCADA Strangelove. His articles were published in HITB Magazine, The Hacker Magazine, and RSDN Magazine. Spoke at conferences and meetups for developers. He is also the co-organizer of Positive Development User Group, a community for developers who are interested in application security.

- Language
- Russian

Head of the application security assessment team. He is engaged in the development of PT Application Inspector being an expert in application security and applied cryptography. He participated in such projects as Nemerle, YAPOET, and SCADA Strangelove. His articles were published in HITB Magazine, The Hacker Magazine, and RSDN Magazine. Spoke at conferences and meetups for developers. He is also the co-organizer of Positive Development User Group, a community for developers who are interested in application security.


Vladimir Kochetkov

Breaking bad

Author: Gabriel Bergel

Want to visit +14 Tech

The speaker will talk about insecurity of POS and fraud that can you be on. From the classic skimmer, eavesdropping, modification, and installation of third-party software to hardware tampering POS. The report also covers POS security features, main brands, cybercrime, methodology to POS tamper, impacted models, security countermeasures, PCI DSS, EMV, insecurity of EMV and NFC.

- Language
- English

A computer system engineer, currently coursing a Masters in Cybersecurity in the IMF Business School and Camilo José Cela University (Spain). He has 14 years of experience in different fields of information security. He is a speaker at common courses, lectures, workshops, and conferences for information security both nationally and throughout Latin America. Currently, Chief Strategic Officer (CSO) in Dreamlab Technologies, and Chief Security Ambassador in 11Paths.


Gabriel Bergel

Techniques to protect Java apps and ways to bypass them

Author: Philip Lebedev

Want to visit +13 Fast Track

The report outlines a range of protection strategies for Java apps, for most of which there are bypass scenarios available.

- Language
- Russian

A vulnerability research engineer, cryptographer, and information security specialist.


Philip Lebedev

Modern techniques and tools in malware analysis

Author: Ivan Piskunov

Want to visit +13
Hands-on Labs

This hands-on lab will focus on modern countermeasures against malware analysis: anti-debugging techniques, using virtual machines, anti-disassembly tricks, code packing/encryption using current approaches, and special technologies and tools.

- Language
- Russian

Has been working in the IT and IS spheres for more than seven years. He writes on his blog ipiskunov.blogspot.com and in his personal column on SecurityLab.ru. He has written several articles on reversing for The Hacker magazine, and is a resident of the anti-malware.ru portal. His articles were published in magazines and mass media focused on information security, IT audit, and IS department economic management. Has three university degrees: information security, accounting and taxation, and business administration.


Ivan Piskunov

How we hacked distributed configuration management systems

Author: Francis Alexander

Want to visit +13
Tech

The talk deals with how the researchers came across and exploited different configuration management systems during their pentests. The speaker will introduce different distributed configuration management tools, like Apache ZooKeeper, HashiCorp Consul and Serf, CoreOS Etcd; discuss multiple ways to fingerprinting these systems; and exploit generic misconfigurations for increasing attack surface.

- Language
- English

An information security researcher and the author of NoSQL Exploitation Framework. Interested in web app and stand-alone app security, DBMS security, coding tools and fuzzing. Spoke at HITB AMS, Hack in Paris, 44CON, DerbyCon, Defcon.


Francis Alexander

Java Card platform attacks based on malicious applets

Author: Sergei Volokitin

Want to visit +12
Tech

The presentation introduces attacks on the secured containers of a Java-based smart card, which allows an attacker to steal cryptographic keys and PINs of the other applets installed on the card.

- Language
- English

A security analyst at Riscure BV in the Netherlands. Develops new attacks on the Java Card platform installed on the most of the modern smart cards. Received a degree in information security in 2013 and now is working on the Software Science Master program at Radboud University Nijmegen.


Sergei Volokitin

Meet and greet the macOS malware class of 2016

Author: Patrick Wardle

Want to visit +12 Tech

Say hello to KeRanger, Eleanor, Keydnap, and more! 2016 was a busy year for Mac malware authors who released a variety of new macOS malware creations. The talk will provide a technical overview of this malware, by discussing their infection vectors, persistence mechanisms, and features. We will discuss various generic detections that strive to ensure our Mac remain secure.

- Language
- English

Director of Research at Synack. Having worked at NASA and the NSA, and well as presented at many security conferences, he is intimately familiar with aliens, spies, and talking nerdy. In his free time, he collects OS X malware and writes free OS X security tools.


Patrick Wardle

Jumping from a security center to production environments

Author: Oleksandr Kazymyrov

Want to visit +12 Tech

This talk will cover passive (extracting information on assets, users, passwords, private keys, etc.) and active (encrypted credentials) information gathering on a rooted server with an installed security center. Moreover, a method for lateral movement from DMZ to production environments using features of Nessus scanning will be demonstrated. It will help red teams to penetrate deeper into internal networks, especially into those containing highly valuable information, like cardholder data environments. From the blue team perspective, the demonstrated techniques will help better understand the risk of vulnerability scanners placed unattended in DMZ zones.

- Language
- English

Has a PhD and Candidate of Engineering Sciences degree in information security from the University of Bergen and KNURE, respectively. A member of non-functional test group in Financial Services at EVRY; a penetration tester holding CEH (Certified Ethical Hacker) and CES (Certified Encryption Specialist) certificates. A co-author of the Ukrainian standards of block cipher and hash function.


Oleksandr Kazymyrov

IPv6 network reconnaissance

Author: Fernando Gont

Want to visit +12 Hands-on Labs

The Internet Protocol version 6 (IPv6) and the emerging IPv6 deployments somehow change the rules of the “network reconnaissance” game: with the typical 264 addresses per subnetwork, the traditional brute-force approach to address scanning from the IPv4 world becomes unfeasible. This workshop will cover the latest IPv6 network reconnaissance techniques discussed in RFC7707. It will provide an intense IPv6 hacking experience, focusing on hands-on IPv6 network reconnaissance exercises.

- Language
- English

A security consultant and researcher for SI6 Networks. He specializes in the field of communications protocols security, working for private and governmental organizations from around the world. He has worked on a number of projects for the UK National Infrastructure Security Co-ordination Centre (NISCC) and the UK Centre for the Protection of National Infrastructure (CPNI) in the field of communications protocols security. He has written a series of recommendations for network engineers and implementers of the TCP/IP protocol suite, and has performed the first thorough security assessment of the IPv6 protocol suite.


Fernando Gont

Non-signature-based detection of PHP backdoors

Author: Gregory Zemskov

Want to visit +12 Fast Track

The speaker reports about the developed and implemented algorithm of non-signature-based detection of malicious PHP code fragments.

- Language
- Russian

Head of Revisium, a company focused on integrated website security. An IS specialist and developer of free website malware and security scanning tools. A permanent participant of conferences, a lecturer at Moscow State University of Mechanical Engineering, an author of courses, master classes and numerous web app security articles.


Gregory Zemskov

Hacker-machine interface

Author: Brian Gorenc

Want to visit +12 Tech

This talk covers an in-depth analysis performed on a corpus of 200+ confirmed SCADA and HMI vulnerabilities. It details out the popular vulnerability types discovered in HMI solutions developed by the biggest SCADA vendors, including Schneider Electric, Siemens, General Electric, and Advantech. It studies the weaknesses in the technologies used to develop HMI solutions and describes how critical vulnerabilities manifest in the underlying code. The talk will compare the time-to-patch performance of various SCADA vendors, and provide a comparison of the SCADA industry to the rest of the software industry. Additional guidance will be provided to SCADA developers and operators looking to reduce the available attack surface along with a prediction on what we expect next in attacks that leverage SCADA and HMI vulnerabilities.

- Language
- English

A senior manager of Vulnerability Research at Trend Micro. He leads the Zero Day Initiative (ZDI) program, which represents the world's largest vendor-agnostic bug bounty program. His focus includes analyzing and performing root-cause analysis on hundreds of zero-day vulnerabilities submitted by ZDI researchers from around the world. The ZDI works to expose and remediate weaknesses in the world's most popular software. He is also responsible for organizing and adjudicating the ever-popular Pwn2Own hacking competitions.


Brian Gorenc

HummingBad: past, present, and future

Author: Andrey Polkovnichenko

Want to visit +12 Tech

First-hand details on research of one of the most widespread mobile botnets by Check Point specialists. What is HummingBad, what are the perils, what is behind, and how to deal with it.

- Language
- Russian

A reverse engineer team lead at Check Point. For the last three years, he has been saving the world from mobile threats.


Andrey Polkovnichenko

SPONSORS

MEDIA PARTNERS

NATIONAL BANKING JOURNAL

Connect: IT
ИЗДАТЕЛЬСКИЙ ДОМ

ДИРЕКТОР ПО БЕЗОПАСНОСТИ
www.s-director.ru

APPTRACTOR

BIS JOURNAL
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

FORUM'S FRIENDS

STOCKHOLM INTERNATIONAL SUMMIT
4SICS
SECURITY in INDUSTRIAL CONTROL SYSTEMS

hack in the box
Keeping Knowledge Free

POC2013
http://www.powerofcommunity.net

X'con

ConfidEncE 2012

Hack In Paris

iGRIDS

Association RusCrypto

RSDN

AT Consulting

RISSPA
be professional

AIC
Academy of Information Systems

-
-

- About Forum
- News
- Organizer
- Program
- PHD Feedback
- Contacts