



ZERO NIGHTS

2015 25-26 november

25 november

	Track 1	Track 2	Workshop 1	Workshop 2
10.00	Registration			
11.00	Openning			
11.30 12.20	"A praise for hackers", <i>Rodrigo Rubira Branca (BSDaemon)</i>			
12.30 13.20	"Hacking Virtual Appliances", <i>Jeremy Brown</i>	"Hack like a movie star: Step-by-step guide to crafting SCADA payloads for physical attacks with catastrophic consequences", <i>Marina Krotofil</i> "	"Practical Object-Oriented Code Reverse Engineering", <i>Alexander Matrosov, Evgeny Rodionov</i>	"Enlarge your Burp, or How to stop fearing Javadocs", <i>Ivan Yolkin, Igor Bulatenko</i>
13.30 14.20	"Warranty Void If Label Removed - Attacking MPLS Networks", <i>Georgi Geshev</i>	"Modifying the firmwares of industrial switches", <i>Alexander Ermolov</i>		
14.50	Dinner			
16.00 16.50	"Big problems with big data - Hadoop interfaces security", <i>Jakub Kaluzny</i>	"Getting The Most Out Of CSP: a Deep Dive", <i>Sergey Shekyan</i>	"Practical Object-Oriented Code Reverse Engineering", <i>Alexander Matrosov, Evgeny Rodionov</i>	"Enlarge your Burp, or How to stop fearing Javadocs", <i>Ivan Yolkin, Igor Bulatenko</i>
17.00 17.50	"Mathematical theory of input validation vulnerabilities and attacks", <i>Ivan Novikov</i>	"illusoryTLS: Nobody But Us Impersonate, Tamper, and Exploit", <i>Alfonso De Gregorio</i>		"Cross-platform reversing with Frida", <i>Ole André Vadla Ravnås</i>
18.00 19.00	"Cisco IOS shellcode - all-in-one", <i>George Nosenko</i>	"Browser Fuzzing with a Twist (and a Shake)", <i>Jeremy Brown</i>	RuCTF 2015	

	Track 1	Track 2	Workshop 1	Workshop 2
11.00 11.50	"Introducing Choronzon: an approach to knowledge-based evolutionary fuzzing", <i>Nikolaos Naziridis, Zisis Sialveras</i>	"How to build your own Echelon system? Attacks at 3G modems", <i>Timur Yunusov</i>	Defensive Track (20 min) "Correlating security events with Esper", <i>Nikolai Klendar</i> "Analyze it – assembling modern SIEM based on Open Source components for large-scale logs analysis", <i>Daniil Svetlov</i>	"Practical exploitation of AVR MC-based devices", <i>Alexander Bolshev, Boris Ryutin</i>
12.00 12.50	"Samsung SmartTV: how-to to creating insecure device in today's world", <i>Sergey Belov</i>	"EESIL – universal IL (Intermediate Language) for Radare2", <i>Anton Kochkov</i>	"Fighting against Flash 0-day: a hunt for a tainted vector", <i>Andrey Kovalev, Konstantin Otrashkevich, Evgeny Sidorov</i> "Banking Trojans: a look from the new perspective", <i>Alexey Levin</i> "Automation of web applications scanning: experience of Yandex", <i>Eldar Zaitov</i>	
13.00 13.50	"Did you get your token?", <i>Daniel & azure</i>	"S[c]rum is all around. How to stop continuous integration", <i>Andrey Plastunov</i>	"Do-it-yourself banking SDL", <i>Yuri Shabalin</i> "Let's play the game: One more way to perform penetration test", <i>Kirill Ermakov</i>	
14.00	Dinner			
16.00 16.50	"Fix it yourself: resolving UEFI vulnerabilities single-handedly", <i>Nikolaj Schlej</i>	"KNX security or how to steal a skyscraper", <i>Yegor Litvinov</i>	FastTrack (15 min) "Software vulnerabilities of Yota communication equipment", <i>Mikhail Firstov</i> "Distributing the reconstruction of high-level intermediate representation for large scale malware analysis", <i>Alexander Matrosov, Evgeny Rodionov</i> "Hooked browser network based on BeEF and Google Drive", <i>Denis Kolegov, Oleg Broslavsky, Nikita Oleksov</i>	"Practical exploitation of AVR MC-based devices", <i>Alexander Bolshev, Boris Ryutin</i>
17.00 17.50	"Attacking hypervisors using firmware and hardware", <i>Alexander Matrosov</i>	"Extracting the painful (blue) tooth", <i>Matteo Beccaro, Matteo Collura</i>	"What should a hacker know about WebDav? Vulnerability review in WebDav implementations", <i>Андрей Ефимюк, Мухаил Егоров</i> "ORM2Pwn: exploiting injections in Hibernate", <i>Mikhail Egorov, Sergey Soldatov</i> "Knowledge based approach for fast Internet resource discovery or Data Mining in the service of nmap", <i>Sergey Ignatov, Omar Ganiev</i> "Hands on interpreted language obfuscation", <i>Aleksandr Kurilin</i>	"On the way to (wrong) anonymity. Basic techniques of digital contraception and private data hygiene", <i>Vlad Voronkov</i>
18.00 18.50	"Direct X – direct way to Microsoft Windows kernel", <i>Nikita Tarakanov</i>	"The [Real] State of BGP Security", <i>Alexander Asimov, Artyom Gavrichenkov</i>	RuCTFE 2015	
19.00 19.30	Closing			