Veronica **Valeros**, Ing.

Cybersecurity, Research and Network Analysis

✉ vero.valeros@gmail.com ⌂ www.veronicavaleros.com

Karlovo náměstí, 13 Prague, Czech Republic ☎ (+420) 224 357 337

Veronica Valeros is a senior researcher and project leader at the Stratosphere Research Laboratory in the Czech Technical University in Prague. She has more than 9 years of experience in cyber security.

Veronica's research strongly focuses on helping people. She currently specializes in threat intelligence, malware traffic analysis, and data analysis. She has made her career in both industry and academia.

In her current position as a project leader, Veronica helps driving forward the research and development projects, improves processes, and drives the community engagement of the groups she works with. As a senior researcher, Veronica's is responsible for the research, development, and customer support at the Civilsphere project, dedicated to protecting civil society organizations and individuals at risk from targeted digital threats.

Veronica has presented her research at international conferences such as Black Hat, EkoParty, Botconf, Virus Bulletin, Deepsec, and others. She is the co-founder of the MatesLab hackerspace based in Argentina and co-founder of the Independent Fund for Women in Tech. She speaks English and Spanish.

Experience

Project Leader, Stratosphere Laboratory, Dep. Computer Science, ČVUT, Prague, Czechia 2019–Present
Responsible for assisting on project planning and coordination with team members and stakeholders. Overseeing the development of projects to ensure milestones are met. Responsible for improving team performance through reviewing and improvement of processes, infrastructure, communication and team organization.

Senior Researcher, Stratosphere Laboratory, Dep. Computer Science, ČVUT, Prague, Czechia 2018–Present
Responsible for leading on existing and new research encompassing multiple areas from malware execution, honeypots data analysis, and network analysis. Responsible for the development and implementation of software monitoring systems and tools for better data capturing and analysis.

Co-Founder, Independent Fund for Women in Tech 2019–Present
An initiative created for the supporting and empowering women in technology and security.

Co-Founder, MatesLab Hackerspace, Mar del Plata, Argentina 2009–Present

Consultant, Stratosphere Laboratory, Dep. Computer Science, ČVUT, Prague, Czechia 2016–2018
Responsible for assisting in investigations, malware analysis, and malware execution.

Threat Researcher, Cognitive Threat Analytics, Cisco Systems, Prague, Czechia 2013–2018
Responsible for planning, deploying, and running the malware laboratory to capture traffic from malware. Head of the threat research team (<10 people) responsible for hunting, identifying and internally reporting on new cyber threats found through analysis of network traffic. Responsibilities also include cyber threat investigations, outreach activities such as blogging and conferences. Designed and implemented training programs in cyber threat research for junior level. Performed long term mentoring activities involving research projects and conferences presentations.

Consultant, Talsoft S.R.L, Mar del Plata, Argentina 2011–2012
Responsible for assisting in security assessments, customer engagement, testing of new tools, and vulnerability discovery.

Teaching, CEM No. 41, Rio Negro, Argentina 2006–2006
Mathematics Substitute Teacher at CEM no. 41 High School, teaching 3rd, 4th and 5th graders.

Projects

AI-VPN, Stratosphere Laboratory, Dep. Computer Science, ČVUT, Prague, Czechia 2020–Present
This projects focuses on the research and development of a local and easy to implement VPN that checks the traffic of devices with AI-based detection to automatically block threats and stop dangerous privacy leaks. The detection of malicious threats, attacks, infections and private leaked data is implemented using novel free software AI technology.

Civilsphere, Stratosphere Laboratory, Dep. Computer Science, ČVUT, Prague, Czechia 2018–Present

The mission of this project is to provide journalists, activists, and human rights defendants services and tools to early identify digital threats jeopardizing their life and work.

Conectándonos, Fraternity of St. Thomas Aquinas Groups (FASTA), Rio Negro, Argentina 2006–2006
The mission of this project was to train teachers and students in computer technologies, to reduce the technological gap in the educational sector. As a project leader and instructor, we run a successful pilot of this project in an isolated remote high school in Patagonia.

Committees

Organizing Committee Member: WSegI 2010, WSegI 2009

Reviewer: EkoParty 2020, EkoParty 2019, EkoParty 2018, Black Hat EU 2018, BSides Zurich 2018, Black Hat EU 2017, GreHack 2017, BSides Zurich 2017

Education

Computer Engineering (Ing.), Fraternity of St. Thomas Aquinas Groups (FASTA), Argentina 2013
Subject of the dissertation: Análisis de anomalías en protocolos web para la detección de ataques.
Supervisors: Carlos Benitez and Lucía Isabel Passoni and Sebastián García

Mercantile Expert Oriented on Computing, Francisco Pascasio Moreno High School, Argentina 2003

Primary School No. 186, 'El Turbio' nature reserve, Argentina 2000

Primary School No. 41, 'Las Golondrinas' nature reserve, Argentina 1997

Awards

Information Security Undergraduate Scholarship, (ISC)2 Foundation 2011

State Scholarship Grant, Department of Scholarships and Compensation Policies of Chubut Province, Argentina 2010-2011

Student Scholarship, Fraternity of St. Thomas Aquinas Groups (FASTA) 2007-2012

Special Mention, 'Instituto Balseiro' Scholarship 2002 for High School Students 2002
Award to top 50 short monograph about "Education, scientific research and technological development".

Best Technological Project Idea, Ministry of Education of Chubut Province, Argentina 1999
Won the technological project and prototype idea to build a bridge over 'Pedregoso' river at primary school No. 186, nature reserve 'El Turbio'. The bridge was completed in December 1999 and continues in use today.

Courses

Fundamentals of Graphic Design, California Institute of the Arts (Coursera) 2017
Verify at Coursera: coursera.org/verify/BUSWLTWPEHCU

Introduction to Public Speaking, University of Washington (Coursera) 2018
Verify at Coursera: coursera.org/verify/AX9KH3238HVJ

Fundamentals of Visualization with Tableau, University of California, Davis (Coursera) 2018
Verify at Coursera: coursera.org/verify/TNPLU5LHCXLP

What is news?, Michigan State University (Coursera) 2018
Verify at Coursera: coursera.org/verify/2R5DWTBMRE4K

International Cyber Conflicts, The State University of New York (Coursera) 2020
Verify at Coursera: coursera.org/verify/5AJF6QKJMMT2

Teaching

Teaching assistant, Introduction to Computer Security (in English) Fall 2020
Open Informatics Master Program, ČVUT in Prague

Trainer, Black Hat EU 2020 Dec 2020
Official training with Sebastian Garcia: Advanced Malware Traffic Analysis: Adversarial Thinking

Trainer, Black Hat Asia 2020 Sep 2020
Official training with Sebastian Garcia: Advanced Malware Traffic Analysis: Adversarial Thinking

Trainer, Black Hat US 2020 Aug 2020
Official training with Sebastian Garcia: Advanced Malware Traffic Analysis: Adversarial Thinking

Trainer, Ekoparty 2019, Buenos Aires, Argentina Sep 2019
Official training with Sebastian Garcia:Getting Your Hands Dirty: Understanding & Hunting Down Malware Attacks in Your Network

Trainer, Black Hat US 2019, Las Vegas, US Aug 2019
Official training with Sebastian Garcia: Advanced Malware Traffic Analysis: Adversarial Thinking

Trainer, OWASP Czech Republic Conference, Prague, Czechia May 2019
Official training with Sebastian Garcia: Getting Your Hands Dirty: IoT Botnet Analysis

Trainer, Black Hat Asia 2019, Singapore, Republic of Singapore Mar 2019
Official training with Sebastian Garcia: Advanced Malware Traffic Analysis: Adversarial Thinking

Trainer, Troopers, Heidelberg, Germany Mar 2019
Official training with Sebastian Garcia: Machine Learning for Network Security and Malware Detection

Trainer, Internet Freedom Festival, Valencia, Spain Mar 2019
Official training with Sebastian Garcia: Emergency VPN: Analyzing mobile network traffic to detect digital threats

Trainer, Black Hat EU 2018, London, UK Dec 2018
Official training with Sebastian Garcia: Advanced Malware Traffic Analysis: Adversarial Thinking

Trainer, HackLu 2018, Luxembourg, Luxembourg Oct 2018
Official training with Sebastian Garcia: Getting Your Hands Dirty: How to Analyze the Behavior of Malware Traffic and Web Connections

Trainer, EkoParty 2018, Buenos Aires, Argentina Oct 2018
Official training with Sebastian Garcia: Advanced Malware Attacks In Your Network

Trainer, University of Luxembourg, Luxembourg, Luxembourg July 2016
Workshop, Intrusion Detection and NetFlow Analysis

Trainer, Botconf 2016, Lyon, France Nov 2016
Official training with Sebastian Garcia: Getting your hands dirty: How to Analyze the Behavior of Malware Traffic and Web Connections

Trainer, Czech Technical University in Prague, Czechia Oct 2016
Network Analysis for Threat Intelligence

Supervision

Jakub Čech, Master thesis, Faculty of Electrical Engineering, ČVUT in Prague. 2020

Languages

Spanish: Native proficiency

English: Full professional proficiency

Personal interests

Technology, Languages, Wine, Traveling, Communication, Leadership

Publications

Peer-reviewed journals

[1] Make it count: an analysis of a brute-forcing botnet
V. Valeros
The Journal on Cybercrime & Digital Investigations 1.1 (2016)
DOI: 10.18464/cybin.v1i1

[2] An Overview of the WCMS Brute-forcing Malware Landscape
A. Shirokova, V. Valeros
The Journal on Cybercrime & Digital Investigations 3.1 (2017), pp. 20–29
DOI: 10.18464/cybin.v3i1

Peer-reviewed conference proceedings

[1] Educarse y divertirse, la Universidad y el Hackspace
V. Valeros, S. Garcia
V Congreso de Tecnología en Educación y Educación en Tecnología, 2010

[2] De la universidad al hacklab, respetar y divertirse en la educación
V. Valeros, S. Garcia
World Engineering Congress, 2010

[3] Detecting DGA malware using NetFlow
M. Grill, I. Nikolaev, V. Valeros, M. Rehak
2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015
DOI: 10.1109/INM.2015.7140486

[4] Machete: Dissecting the Operations of a Cyber Espionage Group in Latin America
V. Valeros, M. Rigaki, S. Garcia
2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 2019
DOI: 10.1109/EuroSPW.2019.00058

[5] Growth and Commoditization of Remote Access Trojans
V. Valeros, S. Garcia
2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 2020
DOI: 10.1109/EuroSPW51379.2020.00067

Project deliverables and technical reports

[1] ENISA – Encrypted Traffic Analysis: Use Cases & Security Challenges
J. Fajfer, N. Müller, E. Papadogiannaki, E. Rekleitis, F. Střasák, K. Böttinger, S. Garcia, I. Lella, V. Valeros
2019

Presentations

[1] Tapping on the Wire: Understanding Malicious Behaviors on the Network
Black Hat Webcast, 2021

[2] Remote Access Trojans in the Cyber Crime World: Past, Present, and Future
CERT-EU, 2020

[3] Growth and Commoditization of Remote Access Trojans
Virus Bulletin, 2020

[4] Civilsphere's Emergency VPN: Analyzing Mobile Network Traffic to Detect Digital Threats
Internet Freedom Festival Session, 2020

[5] Emergency VPN
Chaos Stage, Chaos Computer Conference 36C3, 2019

[6] Saving the World: Increasing Efficiency and Accuracy of Encrypted Traffic Analysis of People at Risk
OpenAlt, 2019

[7] Spy vs. Spy: A Modern Study Of Microphone Bugs Operation And Detection
BSides BUD (Hungary), 2018

[8] Spy vs. Spy: A Modern Study Of Microphone Bugs Operation And Detection
34C3 (Germany), 2017

[9] Knock Knock... Who's there? admin admin, Get In! An Overview of the CMS Brute-Forcing Malware Landscape
Botconf (France), 2017

[10] América Latina, blanco de un grupo avanzado de cyber espionaje
TandilSec (Argentina), 2017

[11] Panel: Mujeres en Tecnología y Ciencia
UNICEN (Argentina), 2017

[12] Five days in the life of a CMS brute forcing malware
BSides Vienna (Austria), 2017

[13] An overview of the CMS brute-forcing malware landscape
BruCON (Belgium), 2017

[14] A new twist on the APT targeting Latin America
GoSec (Canada), 2017

[15] Spy vs. Spy: A modern study of microphone bugs operation and detection
Hack in the Box (Singapore), 2017

[16] The Future of Cybersecurity Needs You: Here is Why
PyData Berlin (Germany), 2017

[17] Threat Hunting En Masse: The 9 Circles of Evil
Copenhagen CyberCrime Conference (Denmark), 2017

[18] Hunting Them All
Troopers (Germany), 2017

[19] 50 Thousand Needles in 5 Million Haystacks: Understanding Old Malware Tricks to Find New Malware Families
BlackHat EU (UK), 2016

[20] Trickeries of a giant: a long term study on malicious adware networks
Secure PL (Poland), 2016

[21] Threat Hunting En Masse: Challenges And Discoveries
Security Automation World (France), 2016

[22] Adware landscape: what you didn't want to hear
University of Luxembourg (Luxembourg), 2016

[23] The Dark Side of Adware: Malware and Data Exfiltration
BSides Tel Aviv (Israel), 2016

[24] Adware's new upsell: malware
BSides Calgary (Canada), 2016

[25] Insights of a brute-forcing botnet
Security Session (Czech Republic) , 2015

[26] Make It Count: an Analysis of a Brute-forcing Botnet
Botconf (France), 2015

[27] How bluetooth may jeopardize your privacy. An analysis of people behavioral patterns in the street
DeepSec (Austria), 2014

[28] Uncovering your trails Privacy issues of bluetooth devices
Ekoparty (Argentina), 2013