



Dancho Danchev

Bulgaria

 dancho.danchev@hush.com

 +359876893890

 [linkedin.com/in/danchodanchev](https://www.linkedin.com/in/danchodanchev)


Summary

Dancho Danchev is the world's leading expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodology for processing threat intelligence leading to a successful set of hundreds of high-quality analysis and research articles published at the industry's leading threat intelligence blog - ZDNet's Zero Day, Dancho Danchev's Mind Streams of Information Security Knowledge and Webroot's Threat Blog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge which has received over 5.6M page views since December, 2005 and is currently considered one of the security industry's most popular security publications.

- Presented at the GCHQ with the HoneyNet Project
- SCMagazine Who to Follow on Twitter for 2011
- Participated in a Top Secret GCHQ Program called "Lovely Horse"
- Identified a major victim of the SolarWinds Attack - PaloAltoNetworks
- Found malware on the Web Site of Flashpoint
- Tracked monitored and profiled the Koobface Botnet and exposed one botnet operator
- Made it to Slashdot two times
- My Personal Blog got 5.6M Page Views Since December, 2005
- My old Twitter Account got 11,000 followers
- I had an average of 7,000 RSS readers on my blog
- I have my own vinyl "Blue Sabbath Black Cheer / Griefer – We Hate You / Dancho Danchev Suck My Dick" made by a Canadian artist
- Currently running Astalavista.box.sk
- I gave an interview to DW on the Koobface Botnet
- I gave an interview to NYTimes on the Koobface botnet
- I gave an interview to Russian OSINT
- Listed as a major competitor by Jeffrey Carr's Taia Global
- Presented at the GCHQ
- Presented at Interpol
- Presented at InfoSec
- Presented at CyberCamp
- Presented at RSA Europe

He's currently running a high-profile hacking and security project on the original <https://astalavista.box.sk> and can be reached at dancho.danchev@hush.com

Experience

-  **DNS Threat Researcher**
WhoisXML API
Apr 2021 - Present (2 months +)

DNS Threat Researcher - <https://www.whoisxmlapi.com/>



Project Operator

Astalavista.box.sk

Jan 2020 - Present (1 year 5 months +)

<https://astalavista.box.sk>



Threat Intelligence Analyst

GroupSense

Sep 2020 - Feb 2021 (6 months)

Threat Intelligence Analyst - <https://groupsense.io/>



Security Blogger

Nov 2019 - Dec 2019 (2 months)

Security Blogger at Armadillo Phone - <https://www.armadillophone.com>



OSINT Analyst

Treadstone 71

Jan 2019 - Jun 2019 (6 months)

OSINT Analyst at Treadstone71 - <https://www.treadstone71.com/>



Security Consultant

KCS GROUP EUROPE LIMITED

Apr 2018 - Jul 2018 (4 months)

Security Consultant - <https://www.kcsgroup.com/>



Threat Intelligence Analyst

GroupSense

Jan 2017 - Mar 2017 (3 months)

Threat Intelligence Analyst - <https://groupsense.io/>



Security Consultant

Wandera

Nov 2014 - Jan 2015 (3 months)

Security Consultant at Wandera - <https://www.wandera.com/blog/>



Security Blogger

Webroot

Jan 2012 - Jun 2014 (2 years 6 months)

Security blogger and cybercrime researcher at the industry's leading cyber threat intelligence blog - <http://webroot.com/blog>



Security Blogger

ZDNet

May 2008 - Feb 2013 (4 years 10 months)

Covering the very latest in the world of cyber security - <http://www.zdnet.com/blog/security>



Managing Director - Astalavista.com

ASTALAVISTA IT Engineering GmbH

Mar 2003 - Jun 2006 (3 years 4 months)

Managing Director - Astalavista Security Group's - Astalavista.com - <https://packetstormsecurity.com/groups/astalavista>



Security Consultant

TechGenix

Jun 2003 - Jan 2005 (1 year 8 months)

Security Consultant at TechGenix's WindowSecurity.com - <http://techgenix.com/author/dancho-danchev/>



Technical Collector

LockDownCorp

Jan 2000 - Dec 2003 (4 years)

Technical Collector of Trojans/Worms/Viruses/VBS Scripts for LockDownCorp - <http://www.lockdowncorp.com/>



Security Consultant

Frame4 Security Systems

Jan 2002 - Dec 2002 (1 year)

Security Consultant and Editorial Writer for Frame4 Security Systems - <http://frame4.com> the author of "The Complete Windows Trojans Paper" - https://packetstormsecurity.com/files/17526/comp_trojans.txt.html



Trojan Information Database Manager

DiamondCS

Jan 1999 - Dec 1999 (1 year)

Newsletter Manager and Trojan Information Database Manager for DiamondCS's- <http://tds.diamondcs.com.au> - Trojan Defense Suite - <https://packetstormsecurity.com/files/25533/tlibrary.zip.html>

Education



Hogeschool Inholland / Inholland University of Applied Sciences

Bachelor's degree, International Business and Management Studies

2003 - 2006



Zuyd Hogeschool | Zuyd University of Applied Sciences

Skills

Information Security • Publishing • Blogging • Fraud Investigations • Network Security • IPS • Investigative Research • Incident Response • Encryption • Security

Honors & Awards



Jessy H. Neal Award - ZDNet - Zero Day's Blog - 2010 - Jessy H. Neal Award

Jan 2010

Jessy H. Neal Award - ZDNet - Zero Day's Blog - 2010 - <https://www.zdnet.com/meet-the-team/us/dancho-danchev/>



SCMagazine - Who To Follow on Twitter - 2011 - SCMagazine

Jan 2011

SCMagazine - Who To Follow on Twitter - 2011 - <https://www.scmagazine.com/home/opinions/blogs/the-sc-magazine-awards-blog/2011-sc-social-media-awards-finalists-named/>