

Cyber

Intelligence

**The Definite Cybercrime and Web 2.0 Memoir
Courtesy of Dancho Danchev**

The RBN, The Koobface Botnet, The Rock Phish Gang,
Spam Phishing and Malware Campaigns Including Botnet and
Money Mule Recruitment Scams Traced Down to Their
Source Including Various Underground Market Propositions
Exposed

<https://ddanchev.blogspot.com>

Dancho Danchev

Cyber Intelligence by Dancho Danchev

Cyber Intelligence

Copyright © 2021 by Dancho Danchev

First edition

All rights reserved. No part of this publication may be reproduced, stored or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without written permission from the publisher. It is illegal to copy this book, post it to a website, or distribute it by any other means without permission.



Welcome to the wonderful world of cybercrime research threat intelligence gathering and security blogging.

This is Dancho Danchev (<https://ddanchev.blogspot.com>) and I'm proud to let you know that I've finally managed to release my personal memoir which basically details my story as a hacker enthusiast during the 90's up to present day where I'm an internationally recognized cybercrime researcher security blogger and threat intelligence gathering analyst that's running one of the security industry's most popular security publication which is my personal blog since December, 2005 when I was studying in the Netherlands while working and running the infamous - <https://astalavista.com> portal where I was busy acting as a Managing Director and where I was primarily responsible for managing the Security Directory and the Security News sections including the production of the Security Newsletter where I was busy featuring an exclusive and never-published before security interview with a key individual from the Scene and the security industry on a monthly basis.

Table of Contents

Introduction

Dedication

Foreword

Biography

Special Thanks

Testimonials

My Personal Blog

The Hacker Enthusiast Years - The 90's

Early Stage Career - The 90's

OSINT Career Experience

Webroot Experience

Astalavista.com Experience

Security Interview - Part One

Security Interview - Part Two

Lovely Horse Participation

Koobface Investigations

Bonus Content - Visiting GCHQ

Interpol Conference Visit

RSA Europe 2012 Conference Visit

InfoSec 2012 Conference Visit

Bonus Content - ZDNet Articles

Bonus Content - Webroot Research

Bonus Content - WhoisXML API Research

Cyber Intelligence by Dancho Danchev



Dear readers,

This is Dancho and it's a pleasure and an honor to introduce you to my personal E-Book including paperback memoir which aims to details my story as a hacker enthusiast circa the 90's up to present day where I'm one of the world's most popular security bloggers threat intelligence analyst and cybercrime researchers internationally where I'm currently running one of the security industry's most popular security publications which is my personal - Dancho Danchev's Blog - Mind Streams of Information Security Knowledge publication which has managed to attract approximately 5.6M page views since it's original start in December, 2005 where I was studying in the Netherlands and I was busy working on and running the infamous <https://astalavista.com> portal while I busy acting as a Managing Director of the portal where I was busy responsible for all the content and for attracting new advertisers.


Cyber Intelligence by Dancho Danchev

Following a successful career as a hacker enthusiast during the 90's and a successful management and operation of one of the World's leading portals for hackers and security experts which is <https://astalavista.com> for a period of three years circa 2003-2006 when I originally decided to launch one of the security industry's leading publication which is my personal blog - <https://ddanchev.blogspot.com> I managed to somehow land a successful career as an independent contractor in the world of security blogging cybercrime research and threat intelligence which led me to visit several invite-only conferences including to present at event at an undisclosed location including to actually attract and retain approximately 6M page views which is not necessarily bad for a man one operation in terms of running and maintaining my personal blog for a period of 12 years.

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

Cyber Intelligence by Dancho Danchev



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>

Cyber Intelligence by Dancho Danchev


My current and past positions include: A Member to WarIndustries (<http://warindustries.com>) List Moderator at BlackCode Ravers (<http://blackcode.com>) Contributor Black Sun Research Facility (<http://blacksun.box.sk>) (BSRF) List Moderator Software Contributor (TDS-2 Trojan Information Database) (<https://packetstormsecurity.com/files/25533/tlibrary.zip.html>) DiamondCS Trojan Defense (<http://tds.diamondcs.com.au>) Contributor to LockDownCorp (<http://lockdowncorp.com>) Contributor to HelpNetSecurity (<http://forbidden.net-security.org>)

 **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>

Cyber Intelligence by Dancho Danchev

A Security Consultant for Frame4 Security Systems (<http://frame4.com>)
Contributor to TechGenix's WindowSecurity.com
(<http://www.windowsecurity.com/authors/dancho-danchev/>) Technical
Collector - LockDownCorp - (<https://lockdowncorp.com>) Managing Director -
Astalavista Security Group - (<https://astalavista.com>) Security Consultant -
Wandera - (<https://wandera.com>) Threat Intelligence Analyst - GroupSense -
(<https://groupsense.io>) Security Consultant - KCS Group Europe -
(<https://kcsgroup.com>) OSINT Analyst - Treadstone71 -
(<https://treadstone71.com>) Security Blogger - Armadillo Phone -
(<https://armadillophone.com>) Security Blogger for ZDNet
(<http://www.zdnet.com/blog/security/>) Threat Intelligence Analyst for Webroot
(<https://www.webroot.com/blog/>)

Cyber Intelligence by Dancho Danchev



1

Among the primary reasons for coming up with this 97 pages long personal memoir is to empower fellow researchers and security experts including the general public with an in-depth personal account overview of my experience in the security industry's as a teenage hacker enthusiast back in the 90's today's most popular and often cited security blogger threat intelligence analyst and cybercrime researcher internationally and to present a diverse set of high-quality and never-published and discussed before case studies and enriched technical information and OSINT data on current and emerging cyber attack trends.

Cyber Intelligence by Dancho Danchev



The primary goal of the book would be to position my memoir as one of the most popular and often cited personal account of the hacking and the security Scene circa the 90's through the prism of my teenage hacker experience up to present day in terms of various high-profile and advanced nation-state actors and malicious and fraudulent cyber attack campaigns where the ultimate goal would be to discuss in-depth my experience in the field of security blogging threat intelligence gathering and cybercrime research throughout the past decade.

Cyber Intelligence by Dancho Danchev

It used to be a moment in time when “sharing was caring” and with the booming Web 2.0 enterprises and the actual concept numerous new online participants and Web 2.0 darlings started popping up as mushrooms another set of individuals prone to make a change an impact quickly emerged online potentially sharing a treasure trove of personal knowledge into the world of modern technologies including the very basics of information security hacking and cyber warfare including a newly releases and never-published before research into the area of cybercrime research and the actual process of profiling the bad guys online in terms of their actual campaigns and actual malicious infrastructure behind their online campaigns.



The primary goal of the book would be to position my memoir as one of the most popular and often cited personal account of the hacking and the security Scene circa the 90's through the prism of my teenage hacker experience up to present day in terms of various high-profile and advanced nation-state actors and malicious and fraudulent cyber attack campaigns where the ultimate goal would be to discuss in-depth my experience in the field of security blogging threat intelligence gathering and cybercrime research throughout the past decade.

Cyber Intelligence by Dancho Danchev

It used to be a moment in time when “sharing was caring” and with the booming Web 2.0 enterprises and the actual concept numerous new online participants and Web 2.0 darlings started popping up as mushrooms another set of individuals prone to make a change an impact quickly emerged online potentially sharing a treasure trove of personal knowledge into the world of modern technologies including the very basics of information security hacking and cyber warfare including a newly releases and never-published before research into the area of cybercrime research and the actual process of profiling the bad guys online in terms of their actual campaigns and actual malicious infrastructure behind their online campaigns.



Following a series of messages left on the actual C&C (Command and Control) server locations which were basically greeting me and referencing my research at the time including a series of typosquatted domains using my name at some point in time I managed to actually come up with a proper “Top 10 Things You Didn’t Know About the Koobface Gang” article for ZDNet at the time wheret the botnet masters actually left a message within the C&C (Command and Control) server location basically answering the key points on a point by point basis which was quite a success at the time of monitoring and tracking down the Koobface botnet.

Cyber Intelligence by Dancho Danchev

The primary purpose behind the actual release of my personal memoir is to reach out to a new set of audience and actually elaborate more on my experience and expertise in the field including to offer a God's Eye perspective on the current and emerging cybercrime ecosystem in combination with active case studies and technical material whose purpose is to greatly assist everyone that's reading this memoir with the idea to provoke you to share it with your friends and colleagues including to actually recommend it to your friends and colleagues.

CC info	Auth code	Auth result	Amount	Void	Merchant location	Brand	Type	Level	Rank	Rank extra (*)	Country
444392	000000	00	Approved	4.75	OK	15225 KVILLE OHENY PITTSBURGH	VISA	DEBIT	PREPAID	SUTTONBANK	UNITED STATES
474472	008915	00	Approved	3.53	OK	36114 ALBANY CONWAY KONT COMERY	VISA	DEBIT	CLASSIC	BANK OF AMERICA N A	UNITED STATES
43425	09112	00	Approved	2.35	OK	86054 AZNAWAJO SHONTO	VISA	DEBIT	CLASSIC	WELLS FARGO BANK N A	UNITED STATES
5215	0291	00	Approved	8.18	OK	87302 HMOBOLALAGUNA	MASTERCARD	DEBIT	STANDARD	SECURITY SERVICE FEDERAL CREDIT UNION	UNITED STATES
438	062	05	Decline	3.25	---	04046 ME YORK LIMERICK	VISA	CREDIT	CLASSIC	JPMORGAN CHASE BANK N A	UNITED STATES
43425	00114	14	Card No. Error	3.88	---	04217 ME OXFORD DETI EEL	VISA	DEBIT	CLASSIC	WELLS FARGO BANK N A	UNITED STATES
441185	000000	00	Approved	5.95	OK	24333 VA GALAX CITY GALAX	VISA	DEBIT	CLASSIC	JPMORGAN CHASE BANK N A	UNITED STATES
4147	060	05	Decline	8.93	---	16025 PA BUTLER CHICORA	VISA	CREDIT	CLASSIC	JPMORGAN CHASE BANK N A	UNITED STATES
474472	009400	00	Approved	4.32	OK	62008 CA SAN DIEGO ESCOBODO	VISA	DEBIT	CLASSIC	BANK OF AMERICA N A	UNITED STATES
41470	07903	00	Approved	5.98	OK	68382 ME OTTOE LORTON	VISA	CREDIT	CLASSIC	CAPITAL ONE BANK USA N A	UNITED STATES
5424	0619	00	Approved	5.41	OK	98571 WA GRAYS HARBOR PACIFIC BEACH	MASTERCARD	CREDIT	PLATINUM	DTBANK N A	UNITED STATES
440303	000000	01	Decline	8.15	---	88101 CO ARAPAHO LITTLETON	VISA	DEBIT	PREPAID	SUTTONBANK	UNITED STATES
414	155	05	Decline	3.75	---	34822 OR OREGON TIRIBAWK	VISA	CREDIT	CLASSIC	AMERICAN CHASE BANK N A	UNITED STATES
43425	00000	00	Approved	3.79	OK	12542 NY PALM BEACH PALM BEACH	VISA	DEBIT	CLASSIC	WELLS FARGO BANK N A	UNITED STATES
425247	000000	00	Approved	3.78	OK	81542 IL JOLIET ILL JOLIET OHN	VISA	DEBIT	CLASSIC	REGIONS BANK	UNITED STATES
43425	0815	00	Approved	2.58	OK	87388 OR WALHELEA PROSIDE	VISA	DEBIT	CLASSIC	WELLS FARGO BANK N A	UNITED STATES

Statistics:
[18] Card No. Error: 1 (0%)
[21] Decline: 1 (0%)
[03] Approval: 11 (68%)
[03] Decline: 3 (18%) (showout 50%)

I wanted to take the time and effort to dedicate this book to my ex-girlfriend circa the 90's Yordanka Ilieva with whom I worked on the infamous <https://astalavista.com> where I had the privilege to work on the infamous Astalavista Security Group Security Newsletter and received the necessary support and guidance in the context of making this high-quality security publication happen including everyone in the U.S that I know and have worked with in the context of fighting cybercrime where I wanted to say big thanks to everyone who ever approached me and said "keep up the good work" and "keep it coming" in the context of motivating me to continue doing my research and continue to publish high-quality research articles and proper cyber threat actor attribution research and analysis including the following people:



Cyber Intelligence by Dancho Danchev

- Ivan Schmid - for being the coolest boss ever in the world and for welcoming me on board at one of the Web's most popular Web site for hackers circa 2003-2006 where I had the privilege to work as a Managing Director of the portal with my ex-girlfriend circa the 90's - Yordanka Ilieva while I was studying in the Netherlands.
- Pascal Mittner - for being the second coolest boss ever in the world who I never really had the chance to meet personally but was properly doing my work and where I was actually getting paid to do my work
- Gary Scott - with whom I had the privilege to exchange data and information during the 90's on my way to produce a high-quality newsletter and actually threat intelligence type of brief for ScanSafe at the time which later on got acquired by Cisco
- Gadi Evron - for keeping it cool and for keeping the spirit and actually inspiring me to do my research while I was busy watching one of his personal presentations at a major security event circa the 90's where he had the opportunity to present
- Paul Ferguson - for keeping it cool and for keeping in touch and for actually inspiring me to do my research into the field of cybercrime research through his daily publications at his personal blog
- Alex Eckelberry - for keeping it cool and corporate and for actually inspiring me to do my research in the field of cybercrime research and for running and maintaining Sunbelt Software which greatly inspired me to do my research in the field of cybercrime research
- Mark Rash - for keeping it cool and for inspiring me to do my research into the field of cybercrime research with his column at SecurityFocus
- Jamie Riden - for being a good professional and someone that I trust and know and for assisting me in several occasions to do my research and continue doing my research
- Steve Santorelli - for personally inviting me to attend an invite-only event and for keeping in touch and for keeping it cool and for personally writing me a personal recommendation based on my research and experience in the industry

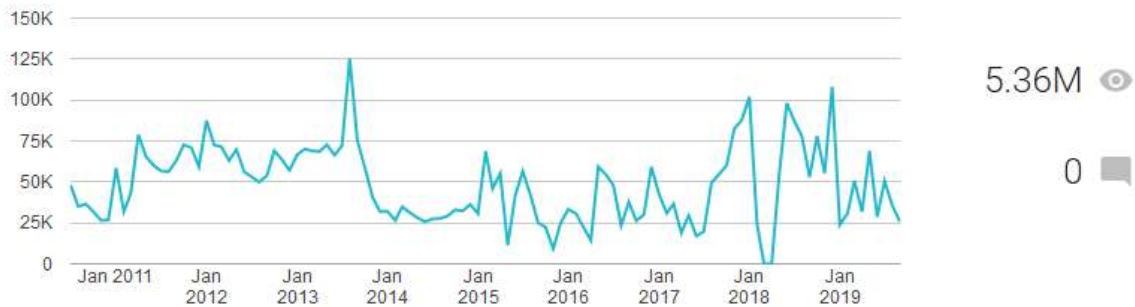
Cyber Intelligence by Dancho Danchev

- James McQuaid - for being among the few individuals to actually raise awareness on the existence of the Russian Business Network and for continuing to supply high-profile and high-value threat intelligence information on a variety of mailing lists
- Jeffrey Bardin - for inviting me to join Treadstone71 as an OSINT Analyst and to actually allow me to work with him on a several projects where I actually earned the necessary amount to pay some of my bills and properly invest in several projects including to launch one of the first commercial E-Shops for intelligence deliverables
- Jeffrey Carr - for keeping it cool and for expressing his personal gratitude and commenting on my research in the context of “keeping it coming”. - Ken Dunham - for keeping it cool and for running a high-profile and popular mailing list for security trends and actual technical information on current and ongoing cyber attack trends
- Jart Armit - for keeping it cool and for approaching me several times to say “hi” and “keep up the good work”
- Robert McMillan - for being a true professional and a good friend with whom I had the privilege and speak and communicate on a numerous occasions
- Rob Lemos - for being a good professional and someone that I know and have worked with and whose work I've followed in the past
- Gregg Keizer - for being a true professional and for actually bothering to quote me and reference me in several articles on numerous occasions - Gary Warner - for being a true professional and for being always on the front lines of fighting the bad guys and cybercrime internationally
- Jorge Mieres - for being a true threat intelligence and cybercrime research professional and for keeping it cool in terms of new research and for offering a unique and in-depth overview and perspective on new and novel cyber attack trends and threats
- Marcus Sachs - for keeping it cool and for being a true professional whose work I've followed in the past
- Gunter Ollman - for being a true professional and a good friend with whom I actually got the chance to meet at RSA Europe 2012 The World is small and infinite and we can definitely make it a better place by doing our work following the basic methodology that an “OSINT conducted today is a tax payer's buck saved somewhere”.

Cyber Intelligence by Dancho Danchev

Dancho Danchev's Blog - Mind Streams of Information Security Knowledge

Views



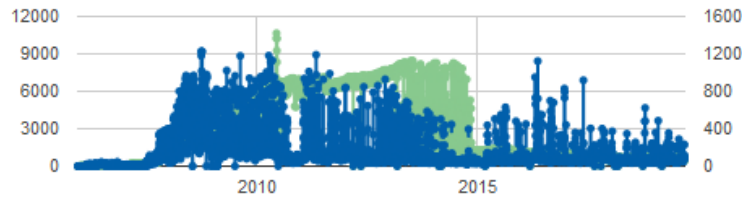
It used to be a privilege back in December, 2005 when I originally launched my personal Dancho Danchev'Blog - Mind Streams of Information Security Knowledge which quickly emerged as one of the security industry's most popular security publications up to present day where I've managed to attract approximately 5.6M page views throughout the past decade and where I've managed to attract and retain a high-quality audience which basically consists of security researchers members of the U.S Intelligence Community including U.S Law Enforcement including prominent members of the security industry where my personal blog became a daily read for the purpose of setting up the foundations of a successful communication platform for most of the research that I publish online.

Following approximately a decade of active security blogging OSINT analysis and research including threat intelligence research and analysis I've managed to gather a loyal audience which greatly contributed to my 11,000 Twitter followers count using my old Twitter account - <https://twitter.com/danchodanchev> including the active participation of my old Twitter account in a Top Secret GCHQ Program known as "Lovely Horse" where I had the privilege to contribute with knowledge and know-how to the U.S Intelligence Community's project for using "Open Source for Security" where the ultimate goal was to monitor high-profile hackers and security experts in terms of obtaining access to their research and knowledge.

Cyber Intelligence by Dancho Danchev

Feed Stats Dashboard

Show stats for all time



Wednesday, December 14, 2005 – Saturday, September 14, 2019

♦ **2,888** subscribers (on average) ⓘ

♦ **157** reach (on average) ⓘ

[See more about your subscribers »](#)

Popular Feed Items

NAME	VIEWS	CLICKS
Total	1,557,394	6,377,221
Historical OSINT - Malicious Malvertising Campaig...	1463	71028
Historical OSINT - Massive Black Hat SEO Campaign...	1397	70766
Historical OSINT - Google Docs Hosted Rogue Chrom...	1402	70669

[See more about your feed items »](#)

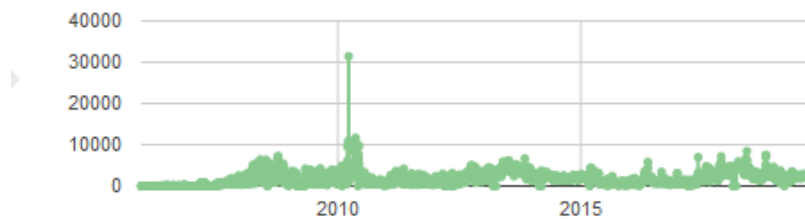
Throughout the past decade it's been a personal privilege and an honor to produce hundreds of high-quality and never-published before high-quality cybercrime research and OSINT type of articles where I'm proud to find out that countless and numerous online publications and security and research journals including mainstream security news outlets have referenced or actually written an article about my research and actual research findings.

Cyber Intelligence by Dancho Danchev

It used to a moment in time when Digg including Techmeme and let's don't forget Technorati were among the primary sourced of traffic and actual content aggregators and syndicating services online which greatly inspired me and motivated me to launch a personal blog which later on became the security industry's leading and most high-traffic visited and popular security publications online. In that specific moment in time when I originally launched my personal blog daily blogging and actual security research was a daily routine which greatly contributed to the popularity of my personal blog in terms of traffic and the actual acquisition of high-profile and loyal readers across the years which is where I've decided to launch my personal Dancho Danchev's Blog - Mind Streams of Information Security Knowledge blog.

Aggregate Item Use

Show stats for



Wednesday, December 14, 2005 – Saturday, September 14, 2019

- ♦ **2,572,020 views** of 1038 items
- ♦ **6,497,440 clicks** back to the site on 1217 items

Cyber Intelligence by Dancho Danchev



It used to be a perfect moment in time when everything was just beginning to take place in the world of hacking in particular the resurrection and re-emergence of key hacking and security resources and online portals online offering vast access to training and teaching documents and text files including actual security and hacking tools which be easily utilized for both defensive and offensive purposes both for educational purposes only.



Cyber Intelligence by Dancho Danchev

With major scene information repositories and hacking sites going down the landscape greatly re-transformed itself into a commercial landscape re-transforming the scene the way we know it into a commercial paradise in particular the rise of the Threat Intelligence and Virtual CYBERINT marketplace consisting of thousands of active participants sharing data information and knowledge on current and emerging cyber threats and cyber threat attack vectors including a multitude of nation-state sponsored and tolerated Cyber Threat Actor adversaries successfully running a huge portion of fraudulent and malicious online campaigns and participating in a multi-million dollar underground Cybercrime Ecosystem.

```
--{ BlackCode Ravers Magazine Issue 2 }--  
Home page : http://www.blackcode.com  
Editor of the magazine: THE mAniAc  
themaniac@blackcode.com
```

Table of contents:

```
-----  
1.Editorial  
2.Mirrors of the magazine  
3.Latest News With BlackCode Ravers  
4.How to break your school security  
5.About Virii  
6.Advertising  
7.Trojans Section  
8.For the newbies  
9.Linux Section  
10.Interviews  
11.Final words  
-----
```

1.Editorial

```
-----  
It's me again.This is our second issue.I've changed the  
design and I've added several new things in the newsletter.  
I've also received a lot of e-mails about our magazine.  
People like it and they want more information here.  
The first issue was short one but of course every new  
issue has many new things added in it.  
I'm happy people like it and we have MANY new subscribers every day.  
Also we have much more visitors than before.
```

Cyber Intelligence by Dancho Danchev

The year is 1998 and Progenic's Top 100's has just added yet another hacking group's portfolio such as for instance among my favorite hacking and security resources which included at the time - WarIndustries, System7, Blackcode, Progenic, Web Fringe, Neworder and TechnicalWarfare. What was really taking place within the Scene and the Industry at the time? With new hacking and community projects continuing to pop-up on a daily basis it wasn't largely a surprise that a new generation of novice and amateur hackers was just beginning to take place with vast repositories of tools and tutorials including articles and guides publicly accessible for everyone to take advantage of and most importantly to get in touch with someone and to learn. What did we managed to achieve throughout the past decade in terms of innovation development knowledge and data spreading to thousands of novice and experienced users across the globe? Let's take for instance the Threat Intelligence market segment - a pioneering passive and active virtual SIGINT marketplace with hundreds of groups participating including thousands of malicious and fraudulent online actors utilizing and relying on basic quality assurance and malicious economies of scale type of market-driven factors to scale their cybercrime and fraud-driven operations online prompting a systematic and nation-state driven response to a growing set of economic and financial terrorism type of online activity largely provoked by a specific set of Russian and Eastern European online adversaries. Among my favorite personal Web site bookmarks at the time were the NBA.com including various other X-Files and related UFO-themed video and photo archive type of personal Web sites. Believe it or not among the early basics of Technical Collection that I managed to inquire were through the public and proprietary research published by a company called iDefense which was basically always there to provide the necessary intelligence on current and future cyber groups and current and future cyber actors which greatly inspired me on my way to do my research in the field of OSINT (Open Source Intelligence) and later on Cybercrime Research and Threat Intelligence gathering. Who were the hackers and what were they up to? What tools did they use? How famous were they at the time? How did they manage to achieve all of this? Remember the U.S-China crashed airplane skirmish? If it's going to be massive it better be good

Cyber Intelligence by Dancho Danchev

What this incident clearly showcased at the time is the possible offensive cyber warfare scenario where U.S based and China-based hackers actually popped-up online to defend and actually launch attacks against each other potentially signifying one of the first major international cyber incidents at the time. With TextFiles.com additions continuing to pop-up among the first and most notable sections that truly made me an impression and actually inspired me to get involved in the world of Hacking and basically the Scene was the Anarchy and Phreaking and Hacking sections next to the daily visits to Progenic.com Top100 list of hacking and security Web sites to actually catch up with the votes and check the new additions to the list to potentially obtain various hacking tools and trojan horses further motivating me to work with them and potentially show them and share them with some of my closest friends of the time circa the 90's for the purpose of attempting to trick irc.dal.net users from various channels including #gay and #lesbians into accepting the latest bogus "screensaver" while exploiting a common flaw in the actual mIRC client where you could easily make it look like that the actual user is receiving an image which in reality was actually an executable part of the server client of a popular trojan horse release at the time.



It used to be a moment in time when “sharing was caring” and with the booming Web 2.0 enterprises and the actual concept numerous new online participants and Web 2.0 darlings started popping up as mushrooms another set of individuals prone to make a change an impact quickly emerged online potentially sharing a treasure trove of personal knowledge into the world of modern technologies including the very basics of information security hacking and cyber warfare including a newly releases and never-published before research into the area of cybercrime research and the actual process of profiling the bad guys online in terms of their actual campaigns and actual malicious infrastructure behind their online campaigns.

Cyber Intelligence by Dancho Danchev

It used to be a personal privilege back in December, 2005 when I originally launched my personal Dancho Danchev's Blog Mind Streams of Information Security Knowledge blog which quickly attracted a high-quality and relevant audience which is currently one of the security industry's most popular and relevant security hacking OSINT and threat intelligence including cybercrime research type of gathering online publications where I've continued to publish and post high-quality and never-published before and released research and analysis articles.

At some point in time I got practically used to getting referenced and quoted by mainstream news media in terms of my research which greatly motivated and inspired me to continue doing my research and to actually attempt to inspire other researchers and readers to continue reading and visiting my blog on a daily basis where I owe everyone a big deal of thanks for the daily visits and for actually bothering to read my articles and actually go through my research at the time up to present day.



Cyber Intelligence by Dancho Danchev

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 in-telligence leading to a successful set of hundreas of high-quality anaysis 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 Web-root'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 Blog - Mind Streams of Information Security Knowledge.

With his research featured at RSA Europe, CyberCamp, InfoSec, GCHQ and Interpol the researcher continues to actively produce threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Se-curity Knowledge publishing a diverse set of hundreds of high-quality research analysis detailing the malicious and fraudulent activities at nation-state and malicious actors across the globe.



Sample public mainstream news media research references and published articles include:

Research and News Articles covering my research and refer-encing me throughout - 2008:

- Russian hacker 'militia' mobilizes to attack Georgia
- Fraudsters Target Facebook With Phishing Scam
- Fake Microsoft e-mail contains Trojan virus

Cyber Intelligence by Dancho Danchev

- Hackers expand massive IFRAME attack to prime sites
- Hackers infiltrate Google searches
- Hackers expand massive IFrame attack to prime sites
- Hackers knocked Comcast.net offline
- Adobe investigates Flash Player attacks
- High-tech bank robbers phone it in
- Attackers booby-trap searches at top Web sites
- Carpet bombing networks in cyberspace
- Storm worm e-mail says U.S. attacked Iran
- India's underground CAPTCHA-breaking economy
- Domain Name Record Altered to Hack Comcast.net
- Google searchers could end up with a new type of bug
- Ongoing IFrame attack proving difficult to kill
- Hackers expand massive IFRAME attack to prime sites
- Danchev: The small pack Web malware exploitation kit
- Danchev: Massive SQL injection the Chinese way
- CAPTCHAs are dead - new research from Dancho Danchev confirms it
- Hackers infiltrate Google searches
- Massive faux-CNN spam blitz uses legit sites to deliver fake Flash
- Faked CNN spam blitz pushes fake Flash
- Danchev: Anti-fraud site DDOS attack
- Sony PlayStation site victim of SQL-injection attack
- Fake CNN Alert Still Spreading Malware
- Look Ma, I'm on CIA.gov

Research and News Articles covering my research and refer-encing me throughout - 2009:

Cyber Intelligence by Dancho Danchev

- “In gaz we trust”: a fake Russian energy company facilitating cybercrime
- Don’t pay your ransom via SMS
- NYT scareware scam linked to click fraud botnet
- Danchev: A crimeware developer’s to-do list
- Danchev rained on my scareware campaign
- Is “aggregate-and-forget” the future of cyber-extortion?
- NYT scareware scam linked to click fraud botnet
- Microsoft declares war on ‘scareware’
- Don’t pay your ransom via SMS
- Twitter warms up malware filter
- What’s really the safest Web Browser?
- With Unrest in Iran, Cyber-attacks Begin
- Zeus bot found using Amazon’s EC2 as C&C server

Research and News Articles covering my research and referencing me throughout - 2010:

- Firefox add-on encrypts sessions with Facebook, Twitter
- Watch out for malware with those pretty Mac screensavers
- Months-old Skype vulnerability exploited in the wild
- Danchev: Money mule recruiters
- Cybercrime’s bulletproof hosting exposed
- Malware Threatens to Sue BitTorrent Downloaders
- Firefox add-on encrypts sessions with Facebook, Twitter
- Chuck Norris Botnet Karate-chops Routers Hard

Research and News Articles covering my research and referencing me throughout - 2011:

- Has EV-SSL Growth Been Slow?
- Report: Vishing Attack Targets Skype Users

Research and News Articles covering my research and referencing me throughout - 2012:

Cyber Intelligence by Dancho Danchev

- Fake UPS notices deliver malware
- ZeuS/Zbot Trojan Spread Through Rogue US Airways Email
- New Skype malware threat reported: Poison Ivy
- Five Koobface botnet suspects named by New York Times
- Virtual jihad: How real is the threat?
- Is the death knell sounding for traditional antivirus?
- Can the Nuclear exploit kit dethrone Blackhole?
- Experts split over regulation for bounty-hunting bug sniffers
- Spammers Using Fake YouTube Notifications to Peddle Drugs
- Adele Bests Adderall As Affiliate Spammers Offer Music Downloads
- Bulgarian sleuth unveils botnet operators
- Fake PayPal Emails Distributing Malware
- Web Gang Operating in the Open
- ZeuS/Zbot Trojan Spread Through Rogue US Airways Email
- Buy 500 hacked Twitter accounts for less than a pint
- NBC.com Hacked, Infected With Citadel Trojan

Research and News Articles covering my research and refer-encing me throughout - 2013:

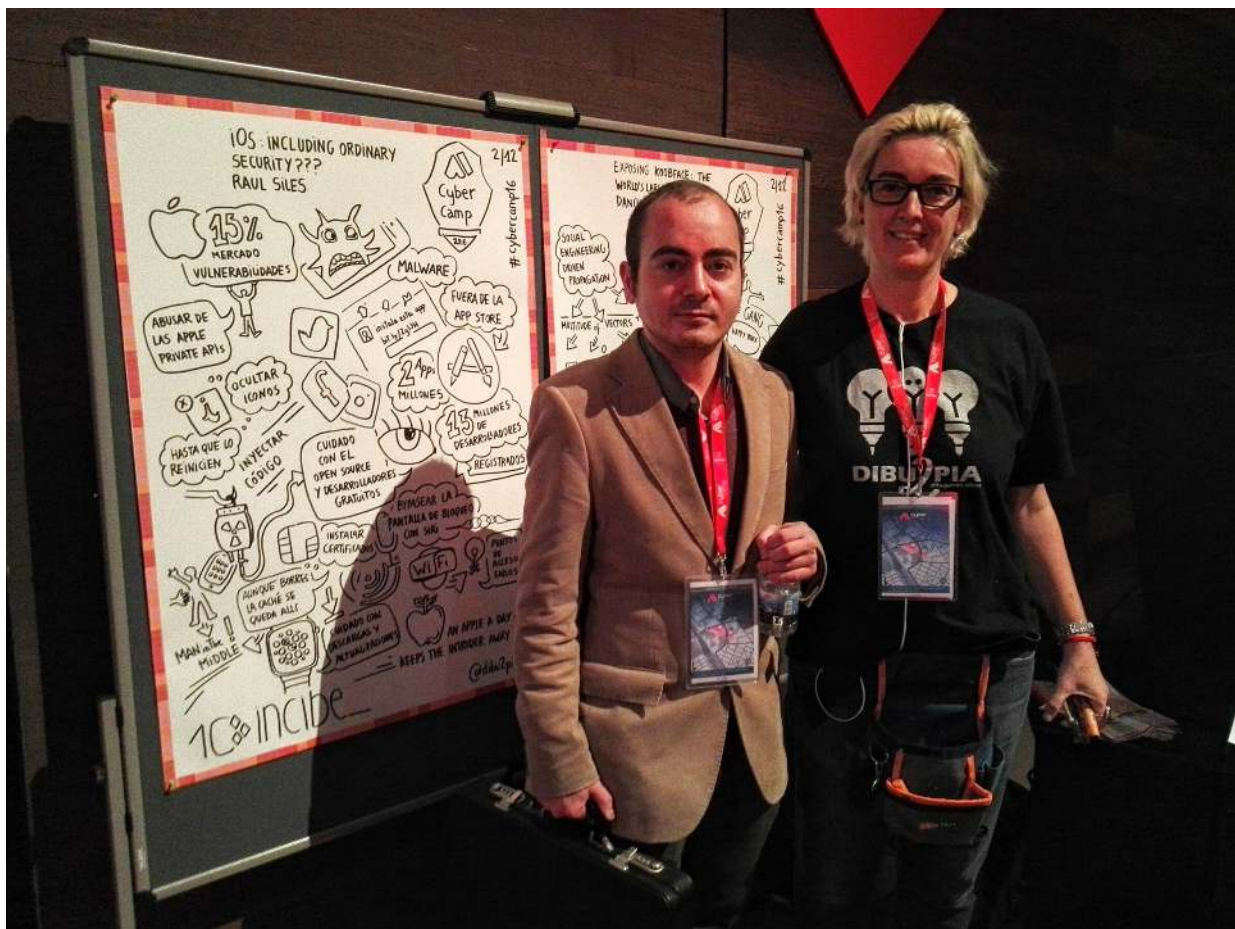
- How Much Does A Botnet Cost?
- Automated YouTube account generator offered to cyber crooks

Cyber Intelligence by Dancho Danchev

- Upgraded Modular Malware Platform Released in Black Market
- Deconstructing the Al-Qassam Cyber Fighters Assault on US Banks
- NBC hack infects visitors in 'drive by' cyberattack
- Bitcoins are being traded for hack tools
- New DIY Google Dorks Based Hacking Tool Released
- Hacking The TDoS Attack
- Mass website hacking tool alerts to dangers of Google dorks
- Cybercrime service automates creation of fake scanned IDs
- Spammers unleash DIY phone number slurping web tool
- Spam email contains malware, not Apple gift card
- APT1, that scary cyber-Cold War gang: Not even China's best
- Mass website hacking tool alerts to dangers of Google dorks
- C&C PHP script for staging DDoS attacks sold on under-ground forums
- Russian Malware-as-a-Service Offers Up Server Rentals for \$240 a Pop
- Java exploit kit sells for \$40 per day
- Buggy DIY botnet tool leaks in black market
- New DIY Google Dorks Based Hacking Tool Released
- Botnets for rent, criminal services sold in the underground market
- Spam email contains malware, not Apple gift card

Cyber Intelligence by Dancho Danchev

It used to be a moment in time when we used to "rock the boat". With or without the drinks. Following a successful career as a hacker enthusiast during the 90's and a successful management and operation of one of the World's leading portals for hackers and security experts which is <https://astalavista.com> for a period of three years circa 2003-2006 when I originally decided to launch one of the security industry's leading publication which is my personal blog - <https://ddanchev.blogspot.com> I managed to somehow land a successful career as an independent contractor in the world of security blogging cybercrime research and threat intelligence which led me to visit several invite-only conferences including to present at event at an undisclosed location including to actually attract and retain approximately 6M page views which is not necessarily bad for a man one operation in terms of running and maintaining my personal blog for a period of 12 years.



Cyber Intelligence by Dancho Danchev

Among the primary reasons for coming up with this 97 pages long personal memoir is to empower fellow researchers and security experts including the general public with an in-depth personal account overview of my experience in the security industry's as a teenage hacker enthusiast back in the 90's today's most popular and often cited security blogger threat intelligence analyst and cybercrime researcher internationally and to present a diverse set of high-quality and never-published and discussed before case studies and enriched technical information and OSINT data on current and emerging cyber attack trends. The primary goal of the book would be to position my memoir as one of the most popular and often cited personal account of the hacking and the security Scene circa the 90's through the prism of my teenage hacker experience up to present day in terms of various high-profile and advanced nation-state actors and malicious and fraudulent cyber attack campaigns where the ultimate goal would be to discuss in-depth my experience in the field of security blogging threat intelligence gathering and cybercrime research throughout the past decade. It used to be a moment in time when "sharing was caring" and with the booming Web 2.0 enterprises and the actual concept numerous new online participants and Web 2





darlings started popping up as mushrooms another set of individuals prone to make a change an impact quickly emerged online potentially sharing a treasure trove of personal knowledge into the world of modern technologies including the very basics of information security hacking and cyber warfare including a newly releases and never-published before research into the area of cybercrime research and the actual process of profiling the bad guys online in terms of their actual campaigns and actual malicious infrastructure behind their online campaigns. It used to be a personal privilege back in December, 2005 when I originally launched my personal Dancho Danchev's Blog - Mind Streams of Information Security Knowledge blog which quickly attracted a high-quality and relevant audience which is currently one of the security industry's most popular and relevant security hacking OSINT and threat intelligence including cybercrime research type of gathering online publications where I've continued to publish and post high-quality and never-published before and released research and analysis articles.

Cyber Intelligence by Dancho Danchev

At some point in time I got practically used to getting referenced and quoted by mainstream news media in terms of my research which greatly motivated and inspired me to continue doing my research and to actually attempt to inspire other researchers and readers to continue reading and visiting my blog on a daily basis where I owe everyone a big deal of thanks for the daily visits and for actually bothering to read my articles and actually go through my research at the time up to present day. Tracking down and monitoring the Koobface botnet on a daily basis where I successfully became the primary source of information on the Koobface botnet at the time was quite a success and a pretty interesting experience where I ultimately managed to take it offline including to hold a Keynote presentation on the topic of monitoring and tracking down of the Koobface botnet



Cyber Intelligence by Dancho Danchev

I originally started my primary area of occupation which is OSINT (Open Source Intelligence) back in December, 2005 when I originally launched my personal blog while studying in the Netherlands and working for - <https://astalavista.com> following and greatly inspired by the infamous "What use are they? They've got over 40,000 people over there reading newspapers." - President Nixon on the CIA in terms of utilizing public and open sources of information for doing research and actually be capable of gathering and working on with intelligence materials. It used to be a moment in time when I originally witnessed the rise of one of the most powerful tools on the Internet which is Google in terms of research compared to a situation approximately over a decade ago when you had to use several different engines at the same time on your way to find valuable information. Today's rise of Google in terms of modern and real-time search technology is an impressive tool in the arsenal of everyone doing research and aiming to gather information and intelligence for their project that also includes the use of the search engine for various OSINT related purposes. OSINT in the context of fighting cybercrime can be best described as the systematic and persistent use of public information for the purpose of building a cyber threat intelligence enriched data sets and intelligence databases both for real-time situational awareness and historical OSINT preservation purposes which also include to actually "connect the dots" in cybercrime gang and rogue cyber actor campaigns and cyber attack type of campaigns. A general example would consist of obtaining a single malicious software sample and using it on a public sandbox to further map the infrastructure of the cybercriminal behind it potentially exposing the big picture behind the campaign and connecting the dots behind their infrastructure which would lead to a multitude and variety of personally identifiable information getting exposed which could help build a proprietary cybercrime gang activity database and actually assist LE in tracking down the prosecuting the cybercriminals behind these campaigns. The primary idea here is to locate free and public online repositories of malicious software and to actually obtain a sample which will be later on used in a public sandbox for the purpose of mapping the Internet-connected infrastructure of the cybercrime gang in question including to actually elaborate more on the ways they attempt to monetize the access to the compromised host including possibly ways in which they make money including to actually find out what exactly are they trying to compromise

Cyber Intelligence by Dancho Danchev

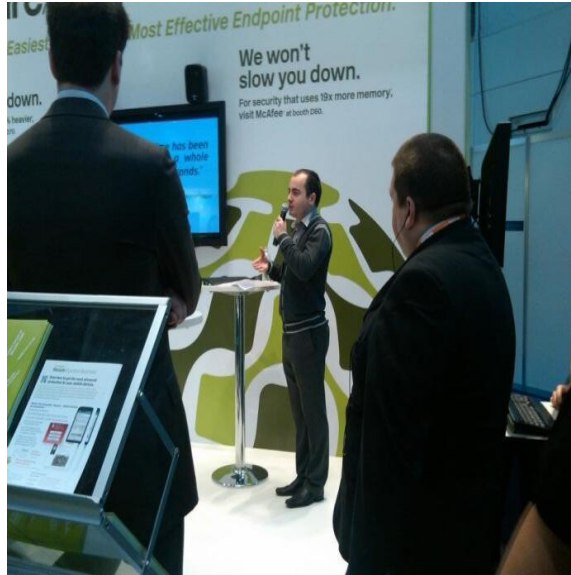
Possible examples here include VirusTotal or actually running a malware interception honeypot such as for instance a spam trap which would allow you to intercept currently circulating in the wild malware campaigns that propagate using email and actually analyze them in terms of connecting the dots exposing their Internet-connected infrastructure and establishing the foundations for a successful career into the world of malicious software analysis and cybercrime research. The next logical step would be to properly assess and analyze the recently obtained sample and to properly establish the foundation of a "connect the dots" culture within your organization where the primary goal would be to have researchers and analysts look for clues on their way to track down and monitor a specific campaign potentially coming up with new and novel cyber attack attribution research. Visualization is often the key to everything in terms of visualizing threats and looking for additional clues and possible cyber attack attribution clues where a popular visualization and threat analysis tool known as Maltego should come into play which basically offers an advanced and sophisticated way to process OSINT and cybercrime research and threat intelligence type of information and actually enrich it using public and proprietary sources of information for the purpose of establishing the big picture and actually connecting the dots for a specific cyber attack campaign. Among the first things that you should consider before beginning your career in the World of OSINT is that everything that you need to know about a specific online event a specific online campaign that also includes the activities of the bad guys online is already out there in the form of publicly accessible information which should be only processed and enriched to the point where the big picture for a specific event or a malicious online campaign should be established using both qualitative and quantitative methodologies that also includes the process of obtaining access to the actual technical details and information behind a specific online event or an actual malicious and rogue online campaign. Among the few key things to keep in mind when doing OSINT including actual OSINT for cyber attack and cyber campaign attack attribution is the fact that in 99% of the cases all the collection information that you need in terms of a specific case is already publicly known and is publicly accessible instead of having to obtain access to a private or a proprietary source of information and the only thing that you would have to do to obtain access to it is to use the World's most popular search engine in terms of collection processing and enrichment

Cyber Intelligence by Dancho Danchev

The second most popular thing to keep in mind when doing OSINT is that you don't need to obtain access to proprietary even public OSINT tools. Following a series of messages left on the actual C&C (Command and Control) server locations which were basically greeting me and referencing my research at the time including a series of typosquatted domains using my name at some point in time I managed to actually come up with a proper "Top 10 Things You Didn't Know About the Koobface Gang" article for ZDNet at the time wheret the botnet masters actually left a message within the C&C (Command and Control) server location basically answering the key points on a point by point basis which was quite a success at the time of monitoring and tracking down the Koobface botnet.



Cyber Intelligence by Dancho Danchev



At a specific moment in time I got a personal invitation for a corporate project to work on using a full-time contract with Webroot Inc which was basically an extremely popular and easy to use and effective endpoint and corporate anti-virus solution where I had the privilege to work as a security blogger for a period of two years where I produced hundreds of high-profile and high-value research analysis on the topic of cybercrime research and malicious software analysis and research which ultimately led to me to visit InfoSec 2012 with my employer where I held several presentations and actually responded to journalist inquiries about our current and ongoing research. Throughout my two years experience while working for Webroot is that I had the privilege to meet some professional folks with whom I had the privilege to work and collaborate including to actually get a pretty good commentary on my research including to actually attend RSA Europe 2012 including InfoSec 2012 on behalf of my employer for the purpose of holding two presentations which were on the basics of Cyber Jihad vs Cyberterrorism including a general overview of trends within the cybercrime ecosystem where I got some pretty interesting questions from folks attending the presentation and actually got the chance and privilege to meet most of the U.S and U.K's team members. I've also managed to produce approximately 1224 pages of blog posts offering and providing actionable intelligence on some of the current and emerging cyber threats at the time which basically consisted of malware spam and phishing campaigns including a general overview of the cybercrime ecosystem in the context of offering additional insight into some of the currently active and in circulation tools of the trade within the cybercrime ecosystem at the time.



Sample Personal Photo of ZDNet's Zero Day Blogger Dancho Danchev.
Imagery courtesy of Dancho Danchev

Cyber Intelligence by Dancho Danchev

The story takes place in a small town in Bulgaria during the 90's in a post Soviet and post Communist country where modern technologies slowly start to take place prompting a local whiz kid to gather as much information from a network of connected computers known as the Internet for the purpose of seeking a global domination through active and persistent information sharing exchange with colleagues from across the globe including exclusively the United States and members of the U.S Security Industry the Scene and prominent members of the U.S Intelligence Community including hundreds of independent contractors in a post and pre 9/11 World which is where Dancho Danchev originally began his career as a hacker enthusiast today's leading expert in the field of cybercrime research and threat intelligence gathering.



Cyber Intelligence by Dancho Danchev

While I was in Bulgaria during my teenage hacker years I was busy freelancing as an information security consultant while working with international security portals where I was busy offering advice and practical information security advice and practical solution recommendations including my work with CIO.bg where I once contributed with an article on Cyberterrorism and Cyber Jihad including a series of publications for HiComm.bg where I was running a popular information security rubric and participated with several articles in several of the magazine's issues.

Dancho Danchev

@danchodanchev

Founder and Chief Executive Officer at Stealth Startup,
Cybercrime Researcher, Security Blogger at Webroot
Inc.

[en.wikipedia.org/wiki/Dancho_Da...](https://en.wikipedia.org/wiki/Dancho_Danchev)

At a later stage I somehow decided to go corporate and in a way find a way to enter the commercial information security industry with my knowledge potentially beginning to contribute with knowledge and information using my personal contacts at various information security portals on my way to land a possible job preferably as a writer security blogger or a journalist which I apparently succeeded in doing as I've been actively contributing with my own research and knowledge on a variety of h/c/p/a (Hacking/Cracking/Phreaking/Anarchy) portals at the time.

At some point in time Dancho decide to approach the primary operator of one of his favorite security Web sites at the time — <https://net-security.org> for the purpose of contributing with an article for their newly launched forbidden.net-security.org project. His idea was to contribute with a security article for their recently launched Newsletter and the article in question was a good old-fashioned “How to use trojan horses” manual. The article eventually got accepted and Dancho felt proud of himself for making a contribution to the project and having his article published so that eventually more people will read it and send him an email with questions about trojan horses and the actual article. The primary Webmaster of net-security.org at the time was Berislav Kucan and the project still remains one of Dancho’s favorite and most popular visited security Web site on a daily basis.



At a later stage I decided to establish a working relationship with Frame4 Security Systems which is a Dutch-based company for the purpose of writing an improved version of the original “How to use trojan horses” paper which later on became the “The Complete Windows Trojans Paper” which quickly became one of the Scene’s most popular and highly read paper on modern trojan horses and how to use them and how to protect against them.

Cyber Intelligence by Dancho Danchev

With the summer coming to an end Dancho got an offer to begin to work at the local office of his ISP (Internet Service Provider) which at the time was Digital Systems for the position of office assistant where he was responsible for introducing new clients to the ISP's service offering and for processing invoices. Among the key benefits for working at the local ISP office was the actual bandwidth that he got access to allowing him to access the Internet without any sort of limitations which he used to visit some of his favorite Top50 and Top100 security and hacking Web sites where he eventually downloaded some of the most recently released hacking and security tools including trojan horses which he copied on a floppy disk and eventually brought back home during the lunch break for the purpose of exchanging the information with his second employer at the time which was an anti-trojans vendor using a publicly accessible FTP server for the purpose of helping his employer improve the detection rate for these type of programs and trojan horses. Dancho would then receive a payment for having collected and actually shared these programs and trojan horses which he would use to pay the bills at the time and actually pay for using his ISP's service.



At some point in time he eventually got approached by a guy known as HeLLfiReZ who was interested in working with him and actually sharing his collection of trojan horses which he would then also share with his employer which at the time was LockDownCorp and earn revenue in the process. It would later come to his attention that the guy that approached him was actually one of the key members of the infamous Sub7 trojan horse group which at a particular point in time was responsible for launching a DDoS (Distributed Denial of Service) attack against the researcher Steve Gibson who extensively profiled the campaign and actually had a conversation with HeLLfiReZ and his team members for the purpose of finding out how launched the attack and how it took place.



He would eventually run a personal hacking and security Web site archive using hosting courtesy of his employer LockDownCorp and run a popular Hacking and Security Web site which he would then feature on Progenic.com's Top100 Hacking and Security Web sites including to actually offer paid security consultations in terms of finding out ways to help people protect their home PCs from trojan horses and teaching them how to use a firewall and how they can secure their home PCs.

Cyber Intelligence by Dancho Danchev

At a later stage in his early Information Security career he would visit and join <https://itsecurity.com>'s Security Clinic where he would have his personal biography featured and actually respond to common security questions which users of the Web site will submit and have his response featured on the front page potentially driving traffic to his employer at the time which was Frame4 Security Systems and actually improving his knowledge and understanding of Information Security in general.

Dancho was also known for having participated in the Blackcode Ravens hacking group which was running the popular <https://blackcode.com> Web site at the time and actually participated with two issues of a popular Security Newsletter at the time which were featured on the home page of the portal.

During the glorious years of IRC (Internet Relay Chat) where Dancho was busy hanging on several IRC networks including DALNet and his local country's IRC network he managed to obtain the `/etc/shadow` password file for his entire ISP (Internet Service Provider) which at the time was Digital Systems and shared a copy of it with his best friend at the time George Kadiyski for the purpose of using several popular and high-profile Wordlists including John the Ripper password cracker potentially obtaining access and brute-forcing the entire password list for hundreds of active dial-up Internet based accounts at the time. Over a period of several days the results at the time were outstanding in the context of actually succeeding in the brute-forcing process potentially allowing Dancho and his friend to easily access free Internet based dial-up accounts which at the time cost money allowing them to use the Internet for free.

At a later stage Dancho also managed to obtain access to his local town's competing ISP (Internet Service Provider) which was known as BIANet `/etc/shadow` which was sent to him by a friend and he also once again shared it with his friend who would once again begin brute-forcing the password file using a variety of Wordlists and the infamous John the Ripper password cracking tool at the time potentially allowing Dancho and his friend easy access to unlimited Internet based dial-up connectivity.



Cyber Intelligence by Dancho Danchev

The time has come to play a game. Dancho quickly powered his 16-bit Pravetz PC 2MB RAM and a screen full of computer game choices quickly appeared prompting him to choose a game. While loading a relatively known game known as Scorch Dancho decided to play two hours and then proceed with meeting his friends and start a discussion with his grandma. A huge fan of strategy games Dancho decided that he didn't have the time to dedicate to play his favorite game — Sid Meier's Civilization and instead he figured that he would eventually play the game later throughout the day. Playing Scorch was quite an experience and he took a few hours of his precious learning time to interact with the game. He then decided to approach his best friend at the time and co-conspirator in the World of UFO's the Soviet Union and computer games including the hacking Scene for two hours of extensive game play where we would strategize on how to best "approach" the Soviet Union in terms of invasion actively and carefully planning every move on our way to invade the Soviet Union and eventually all the surrounding countries. While I was busy preparing for our several hour game play George was supposed to be busy going through a CD which was basically a mirror of Packetstormsecurity in particular the E-Zine section so that we can prepare to have a conversation in terms of working out our technological and military strategy on our way to achieve global domination in the original Sid Meier's Civilization. What we basically did in the beginning was to strategize and actually get a better view of the technology tree of the game and while I was busy moving the Empire along George was busy keeping notes on our way to keep track and advance out military strategy on a "first come first serve" basis.

Cyber Intelligence by Dancho Danchev

Provoked by the need to reach out to a vast network of computers known as the Internet — Dancho quickly decided that the time has come to get connected — so that he decided to seek a proper connection provider in his local home-town. Back in the day the primary connection providers in the time were Bulgaria's Digital Systems BIA Net and the country's leading mobile connectivity provider — Mtel's pre-paid dial-up cards. Times were different in terms of connectivity and DSL and ADSL were a dream come true in the face of corporate networks properly utilizing and using ISDN type of based connectivity. Keeping it simple — Dancho decided to quickly acquire the necessary dial-up modem — which he would eventually fall in love with potentially reaching out to a vast network of computers known as the Internet using the help of a local dial-up provider known as Digital Systems. Back in the day — hourly based dial-up access meant think twice about what you do and how you do it online which means that I would have to basically prepare a plan for the things that I'll do online including Web sites which I would have to visit including a set of emails which I would have to send to a set of people including friends and colleagues.

It's been years since he prepared to acquire a personal computer and get connected meaning that he managed to prepare a list of Web sites and newsgroups on the topic of hacking and computer security including general Web sites that he would eventually visit. Among the first Web sites that he visited was NBA.com where he would quickly learn about the latest developments on his favorite team including daily going through photos and possibly video material to showcase his favorite team at the time. Among the most venerable experienced he first discovered prior to getting connected is to search for UFO photos and information on the KGB including the active reproduction of sound using his external speakers in a MIDI-dominated World at the time. The most venerable and unforgettable experience at the time was the fact that he had access to an email which he used to keep in touch with the Internet Service Provider's system administrator so that he could keep in touch with him including the active sharing of new Web site links for him to visit and exchange communication.

Cyber Intelligence by Dancho Danchev

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Among the first groups which I really joined at the time was Toxic Crisco which basically represented a group of individuals involved in a variety of online activities including possibly hacking including the SCR Project which was basically a social engineering driven hacking group where I was proud to be a member of in particular my active involvement in reading various high-profile psychology books at the time.

For the purpose of using IRC in particular DALnet Dancho quickly gathered a copy of the popular mIRC including several War Scripts ICQ Bombers Nukers and Mail Bombers including trojan horses and quickly decided that he should start getting experienced in the world of hacking for the purpose of gaining knowledge and impressing his friends. Among the first channels that he actually joined at the time were #gay and #lesbian where he was basically portraying himself as another person who was basically seeking to offer a new and novel photos-based screensaver to a variety of individuals for the purpose of tricking them into executing the screensaver on their home PCs ultimately gaining access to their PCs using a popular trojan horse client at the time such as for instance Sub7.

Cyber Intelligence by Dancho Danchev

It would be fairly easy to assume how things got complicated with Dancho quickly obtaining access to Internet Relay Chat's primary mIRC application including a variety of IRC-based "War Scripts" including a dozen of mail-bombers and various other ICQ-based type of Nukers and Flooders on his way to demonstrate a proper technical know-how to his friends and peers in the shady world of hacking. Among the first channels he tried to access were #hacker #hackers #hacking and the infamous #hackphreak on EFNet including to actually open several personal channels on the local IRC networks including #drugs #KGB and #linuxsecurity. At a later stage he actually managed to ask a friend for a possible operator status on the local town's IRC channel where he was basically running a 24/7 online protection bot known as xexploit including the active use of a Socks5 server which at the time was offered by his employer LockDownCorp where he was busy acting as Technical Collector of trojan horses/worms/viruses and VBS scripts for the purpose of improving the anti-trojan software's signatures-based detection rates.

Among the first thing that Dancho decided to do in his spare time is to actively research the local Webmaster of his hometown's official Web site for the purpose of attempting to launch a social engineering attack against his local town's official Web site which basically succeed and resulted in a "greeting" message being posted on the official Web site with no actual data destruction and data removal taking place in what would appear to be a professional approach when compromising a legitimate Web site for the purpose of greeting his personal friends and spread a message on behalf of "Trojan Hacking Group" which at the time basically consisted of one of his closest friends and another fellow hacker enthusiast.

Among his responsibilities the time included the active collection of trojan horses/worms/viruses and VBS Scripts with the idea to share them with his employer which at the time was LockDownCorp one of the world's leading anti-trojan vendors for the purpose of improving the detection rate for these publicly accessible trojan horses in what would later on mature into a successful Technical Collection operation which basically paid his bills and actually offered him a decent financial incentive to continue getting involved in security as a hacker enthusiast and actually improved his employer's overall detection rate for some of the most prolific trojan horses at the time.

Cyber Intelligence by Dancho Danchev

The actual contractual agreement had to do with Dancho housing a private FTP server where he would spend hours uploading collected trojan horses using his home-based dial-up connection and eventually earning a revenue in the process using Western Union where he was happy to have established direct working relationship with one of the world's leading anti-trojans vendors which at the time was located at —

<http://proxy2.stealthedip.com/maniac/incoming/>

Whenever Dancho would attempt to reach out to his friends he would attempt to find out whether they are online using a popular trojan horse including to actually check his email account for their recently changed passwords and other related information including their current IP so that he can properly connect to their home PC for educational purposes.

Being the World's most notable cybercrime researcher security blogger and threat intelligence analyst the researcher quickly gained fame by systematically and efficiently profiling and analyzing a decent snapshot of malicious nation-state and fraudulent activity online leading him to pursue a successful career as the World's most popular cybercrime researcher security blogger and threat intelligence analyst.

In an early Monday morning the researcher quickly gathered a set of research materials of the primary botnet that's he's been monitoring the infamous Koobface botnet using passive and active virtual SIGINT methodologies which basically include active sampling of the botnet's malicious online activities using a daily set of intercepted malicious and fraudulent campaigns launched managed and operated by the Koobface botnet for the purpose of providing the necessary technical operational and strategic OSINT type of intelligence including the daily batch of money mule recruitment domains and campaigns which he was busy profiling with the idea to assist U.S Law Enforcement on its way to track down and prosecute the cybercriminals behind these campaigns.

Cyber Intelligence by Dancho Danchev

The Koobface botnet was the primary botnet propagating over social media at the time in particular Facebook and has already managed to affect tens of thousands of users globally potentially enticing them to interact with rogue and visual social engineering based type of malicious and fraudulent campaigns in the form of Fake Adobe Flash Players and fake YouTube videos where the ultimate goal would be to attempt to affect their friends on Facebook by sending automated and legitimately looking messages including links to rogue and malicious content.

It's been years since he prepared to acquire a personal computer and get connected meaning that he managed to prepare a list of Web sites and newsgroups on the topic of hacking and computer security including general Web sites that he would eventually visit. Among the first Web sites that he visited was NBA.com where he would quickly learn about the latest developments on his favorite team including daily going through photos and possibly video material to showcase his favorite team at the time. Among the most venerable experienced he first discovered prior to getting connected is to search for UFO photos and information on the KGB including the active reproduction of sound using his external speakers in a MIDI-dominated World at the time.

Cyber Intelligence by Dancho Danchev

The most venerable and unforgettable experience at the time was the fact that he had access to an email which he used to keep in touch with the Internet Service Provider's system administrator so that he could keep in touch with him including the active sharing of new Web site links for him to visit and exchange communication. It's been years since he prepared to acquire a personal computer and get connected meaning that he managed to prepare a list of Web sites and newsgroups on the topic of hacking and computer security including general Web sites that he would eventually visit. Among the first Web sites that he visited was NBA.com where he would quickly learn about the latest developments on his favorite team including daily going through photos and possibly video material to showcase his favorite team at the time. Among the most venerable experienced he first discovered prior to getting connected is to search for UFO photos and information on the KGB including the active reproduction of sound using his external speakers in a MIDI-dominated World at the time. The most venerable and unforgettable experience at the time was the fact that he had access to an email which he used to keep in touch with the Internet Service Provider's system administrator so that he could keep in touch with him including the active sharing of new Web site links for him to visit and exchange communication.

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Cyber Intelligence by Dancho Danchev

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Among the first groups which I really joined at the time was Toxic Crisco which basically represented a group of individuals involved in a variety of online activities including possibly hacking including the SCR Project which was basically a social engineering driven hacking group where I was proud to be a member of in particular my active involvement in reading various high-profile psychology books at the time.

Cyber Intelligence by Dancho Danchev

For the purpose of using IRC in particular DALnet Dancho quickly gathered a copy of the popular mIRC including several War Scripts ICQ Bombers Nukers and Mail Bombers including trojan horses and quickly decided that he should start getting experienced in the world of hacking for the purpose of gaining knowledge and impressing his friends. Among the first channels that he actually joined at the time were #gay and #lesbian where he was basically portraying himself as another person who was basically seeking to offer a new and novel photos-based screensaver to a variety of individuals for the purpose of tricking them into executing the screensaver on their home PCs ultimately gaining access to their PCs using a popular trojan horse client at the time such as for instance Sub7.

Among the first groups which I really joined at the time was Toxic Crisco which basically represented a group of individuals involved in a variety of online activities including possibly hacking including the SCR Project which was basically a social engineering driven hacking group where I was proud to be a member of in particular my active involvement in reading various high-profile psychology books at the time.

On a beautiful Thursday afternoon Dancho decided to play a decent computer game while his mother was busy ironing in the kid's room and decided to take a journey successfully getting the World rid of hostile aliens. The game called Duke Nukem basically took Dancho on a journey to another World where he spend most of his afternoon getting rid of evil aliens while he led a discussion with his mother on his whereabouts during the day including active next-day class preparation and the eventual dinner conversation. While mom was busy ironing Dancho took on another journey to a distant World where he took care of and protected the Earth from evil aliens and decided that the time has come for a rest.

Some of the most memorable memories of Dancho back in the time have to do with playing full-time one of the best strategy games during the 90's that's Sid Meier's Civilization. Spending a decent portion of his time basically four hours on a daily basis Dancho quickly acquired the necessary skills to take his civilization to a new level by waging wars developing and exchanging new technologies and by waging wars with competing and adversary civilizations.

Cyber Intelligence by Dancho Danchev

Having already mastered the power of the Civilization game Dancho quickly fell into a World of politics technologies and wars and successfully mapped and left a foothold in the World the way he knew and mastered having successfully spend a decent portion of his time playing the best strategy game during the 90's that's Sid Meier's Civilization. Game World is something different. Whenever Dancho decided to play a game the World came to a halt with Dancho playing and learning the basics and inner workings of every game that he managed to get his hands on throughout the 90's.

Pushing the boundaries of the game at some point Dancho decided to take a deeper look at how you can actually make the computer's player become more advanced and sophisticated and actually tried to train the AI of the game and potentially figured out a way to teach to use advanced warfare tactics.

It would be fairly easy to assume how things got complicated with Dancho quickly obtaining access to Internet Relay Chat's primary mIRC application including a variety of IRC-based "War Scripts" including a dozen of mail-bombers and various other ICQ-based type of Nukers and Flooders on his way to demonstrate a proper technical know-how to his friends and peers in the shady world of hacking. Among the first channels he tried to access were #hacker #hackers #hacking and the infamous #hackphreak on EFNet including to actually open several personal channels on the local IRC networks including #drugs #KGB and #linuxsecurity. At a later stage he actually managed to ask a friend for a possible operator status on the local town's IRC channel where he was basically running a 24/7 online protection bot known as xexploit including the active use of a Socks5 server which at the time was offered by his employer LockDownCorp where he was busy acting as Technical Collector of trojan horses/worms/viruses and VBS scripts for the purpose of improving the anti-trojan software's signatures-based detection rates.

Cyber Intelligence by Dancho Danchev

Among the first thing that Dancho decided to do in his spare time is to actively research the local Webmaster of his hometown's official Web site for the purpose of attempting to launch a social engineering attack against his local town's official Web site which basically succeed and resulted in a "greeting" message being posted on the official Web site with no actual data destruction and data removal taking place in what would appear to be a professional approach when compromising a legitimate Web site for the purpose of greeting his personal friends and spread a message on behalf of "Trojan Hacking Group" which at the time basically consisted of one of his closest friends and another fellow hacker enthusiast.

Among his responsibilities the time included the active collection of trojan horses/worms/viruses and VBS Scripts with the idea to share them with his employer which at the time was LockDownCorp one of the world's leading anti-trojan vendors for the purpose of improving the detection rate for these publicly accessible trojan horses in what would later on mature into a successful Technical Collection operation which basically paid his bills and actually offered him a decent financial incentive to continue getting involved in security as a hacker enthusiast and actually improved his employer's overall detection rate for some of the most prolific trojan horses at the time.

The actual contractual agreement had to do with Dancho using a private FTP server where he would spend hours uploading collected trojan horses using his home-based dial-up connection and eventually earning a revenue in the process using Western Union where he was happy to have established direct working relationship with one of the world's leading anti-trojans vendors which at the time was located at —

<http://proxy2.stealthedip.com/maniac/incoming/>

Whenever Dancho would attempt to reach out to his friends he would attempt to find out whether they are online using a popular trojan horse including to actually check his email account for their recently changed passwords and other related information including their current IP so that he can properly connect to their home PC for educational purposes.

Cyber Intelligence by Dancho Danchev

Being the World's most notable cybercrime researcher security blogger and threat intelligence analyst the researcher quickly gained fame by systematically and efficiently profiling and analyzing a decent snapshot of malicious nation-state and fraudulent activity online leading him to pursue a successful career as the World's most popular cybercrime researcher security blogger and threat intelligence analyst.

Back in 2007 I got a direct invitation to attend a private and invite-only conference event held by the HoneyNet Project at the U.K's GCHQ which I actually attended and presented on a variety of topics including current and emerging cybercrime trends and actually got the opportunity to meet with the folks from the HoneyNet Project.

In 2008 I got a surprise invitation to join the team at ZDNet a web site portal which I greatly admired while I was busy working for <https://astalavista.com> and I was in fact visiting on a daily basis where I spend a highly professional and productive 4 years as a security blogger at ZDNet's Zero Day blog leading to me to thousands of publications including an actual award-winning Jessy H. Neal Award for working on ZDNet's Zero Day blog.

Working for ZDNet greatly shaped my professional well-being in a way that I was basically working with top-notch technology experts from across the globe and actually had the chance to contribute with personal content and research for a period of four years which was an unforgettable experience and it's still a pleasure and a honor to touch base and actually find a way to contribute and say hi to the people that I used to work with back in 2008.

At some point in time I eventually got invited to attend a private and invite-only conference where I presented on money mule recruitment practices and eventually got the privilege to meet most of the people that I work with on a face-to-face basis where we hang out and actually socialized and discussed various hot topics and cybercrime trends internationally.

Cyber Intelligence by Dancho Danchev

Dancho began his career in the world of Intelligence Studies greatly provoked by research published and distributed by a U.S based company known as iDefense which basically specializes in profiling online hacktivism activity and is basically capable of producing high-quality and never-published before threat intelligence and general intelligence briefs. Among the key reports that Dancho was able to get his hands on was the U.S/China skirmish which basically consisted of various U.S and Chinese based groups actively interacting online by launching DDoS (Distributed Denial of Service) attacks against their infrastructure and participating in Web site defacement campaigns. He would then research and actively visit the CIA.gov's official Web site including FAS.org and NSA.gov seeking manuals and research material on Open Source Intelligence (OSINT) which would later on greatly contribute to help him become one of the World's leading experts in the field of cybercrime research and threat intelligence gathering.

In an early Monday morning the researcher quickly gathered a set of research materials of the primary botnet that's he's been monitoring the infamous Koobface botnet. His main motivation behind tracking down and monitoring one of the most prolific botnet that was spreading across Facebook at the time was to assist the Security Industry and researchers internationally including U.S law enforcement on their way to keep track of the botnet's activities and eventually attempt to take it offline and actually attempt to track down some of the authors behind it.

Dancho's daily routine consisted of checking the most recent campaigns launched by the gang and actually offer in-depth technical analysis on the latest campaigns publicly disseminating and profiling the campaigns at his personal blog leading him to a specific set of detailed and in-depth analysis of the Koobface botnet one of the few publicly accessible analysis resources on the topic at the time.

The botnet masters at the time were basically known to keep track of Dancho's research and eventually left a message embedded in the actual C&C infrastructure basically greeting the researcher for his research including a second and a third message during the Christmas season including an actual point-by-point response to his "Top 10 Things You Didn't Know About the Koobface Gang" article which he published at ZDNet's Zero Day blog.

Cyber Intelligence by Dancho Danchev

At a later stage he would present his findings in a Keynote Presentation at CyberCamp 2016 on the topic of “Exposing Koobface — The World’s Largest Botnet” in front of a high-quality audience and actually discuss in-depth how he tracked it down and eventually attempted to take it offline.

While he was busy studying in the Netherlands he became familiar what appeared to be one of the most popular Web sites for hackers on the Web known as Astalavista.com where he managed to actually find the real company behind the portal and actually approached.

In 2021 I can be reached at ddanchev@cryptogroup.net including my personal blog — <https://ddanchev.blogspot.com> including the infamous — <https://astalavista.box.sk> where I’m currently running a high-profile hacking and security project.

The primary purpose behind the actual release of my personal memoir is to reach out to a new set of audience and actually elaborate more on my experience and expertise in the field including to offer a God's Eye perspective on the current and emerging cybercrime ecosystem in combination with active case studies and technical material whose purpose is to greatly assist everyone that's reading this memoir with the idea to provoke you to share it with your friends and colleagues including t

It used to be a moment in time when we used to "rock the boat". With or without the drinks. Following a successful career as a hacker enthusiast during the 90's and a successful management and operation of one of the World's leading portals for hackers and security experts which is <https://astalavista.com> for a period of three years circa 2003-2006 when I originally decided to launch one of the security industry's leading publication which is my personal blog - <https://ddanchev.blogspot.com> I managed to somehow land a successful career as an independent contractor in the world of security blogging cybercrime research and threat intelligence which led me to visit several invite-only conferences including to present at event at an undisclosed location including to actually attract and retain approximately 6M page views which is not necessarily bad for a man one operation in terms of running and maintaining my personal blog for a period of 12 years.



Among the primary reasons for coming up with this 111 pages long personal memoir is to empower fellow researchers and security experts including the general public with an in-depth personal account overview of my experience in the security industry's as a teenage hacker enthusiast back in the 90's today's most popular and often cited security blogger threat intelligence analyst and cybercrime researcher internationally and to present a diverse set of high-quality and never-published and discussed before case studies and enriched technical information and OSINT data on current and emerging cyber attack trends. The primary goal of the book would be to position my memoir as one of the most popular and often cited personal account of the hacking and the security Scene circa the 90's through the prism of my teenage hacker experience up to present day in terms of various high-profile and advanced nation-state actors and malicious and fraudulent cyber attack campaigns where the ultimate goal would be to discuss in-depth my experience in the field of security blogging threat intelligence gathering and cybercrime research throughout the past decade. It used to be a moment in time when "sharing was caring" and with the booming Web 2.0 enterprises and the actual concept numerous new online participants and Web 2

Cyber Intelligence by Dancho Danchev

darlings started popping up as mushrooms another set of individuals prone to make a change an impact quickly emerged online potentially sharing a treasure trove of personal knowledge into the world of modern technologies including the very basics of information security hacking and cyber warfare including a newly releases and never-published before research into the area of cybercrime research and the actual process of profiling the bad guys online in terms of their actual campaigns and actual malicious infrastructure behind their online campaigns. It used to be a personal privilege back in December, 2005 when I originally launched my personal Dancho Danchev's Blog - Mind Streams of Information Security Knowledge blog which quickly attracted a high-quality and relevant audience which is currently one of the security industry's most popular and relevant security hacking OSINT and threat intelligence including cybercrime research type of gathering online publications where I've continued to publish and post high-quality and never-published before and released research and analysis articles. At some point in time I got practically used to getting referenced and quoted by mainstream news media in terms of my research which greatly motivated an inspired me to continue doing my research an to actually attempt to inspire other researchers and readers to continue reading and visiting my blog on a daily basis where I owe everyone a big deal of thanks for the daily visits and for actually bothering to read my articles and actually go through my research at the time up to present day. Tracking down and monitoring the Koobface botnet on a daily basis where I successfully became the primary source of information on the Koobface botnet at the time was quite a success and a pretty interesting experience where I ultimately managed to take it offline including to held a Keynote presentation on the topic of monitoring and tracking down of the Koobface botnet

Cyber Intelligence by Dancho Danchev

Following a series of messages left on the actual C&C (Command and Control) server locations which were basically greeting me and referencing my research at the time including a series of typosquatted domains using my name at some point in time I managed to actually come up with a proper "Top 10 Things You Didn't Know About the Koobface Gang" article for ZDNet at the time where the botnet masters actually left a message within the C&C (Command and Control) server location basically answering the key points on a point by point basis which was quite a success at the time of monitoring and tracking down the Koobface botnet. The primary purpose behind the actual release of my personal memoir is to reach out to to a new set of audience and actually elaborate more on my experience and expertise in the field including to offer a God's Eye perspective on the current and emerging cybercrime ecosystem in combination with active case studies and technical material whose purpose is to greatly assist everyone that's reading this memoir with the idea to provoke you to share it with your friends and colleagues including to actually recommend it to your friends and colleagues.



Cyber Intelligence by Dancho Danchev

Back in the day my primary area of occupation was to monitor and track down the Koobface botnet where I was basically acting as the primary source of real-time and actionable intelligence on the whereabouts of the Koobface botnet including to actually profile and analyze some of their latest campaigns which led to a variety of pretty interesting situations where they've actually redirected Facebook's entire IP space to my personal blog including to actually leave several greetings within the botnet's C&C channel in terms of sending me a message and greeting me including a step by step response to my "Top 10 Things You Didn't Know About the Koobface Gang" article where they actually responded to my ZDNet article at the time in a step by step fashion. At a specific point in time I was originally invited to hold the Keynote presentation at the CyberCamp 2016 security conference where I presented on the topic of tracking down and monitoring the Koobface one of the world's largest botnets which was a tremendous success in the context of communicating most of my research to a wider audience.

C&C ARCHITECTURE

Compared with the complex C&C architecture of the Storm, WALEDAC, and DOWNAD botnets, the KOOBFACE C&C infrastructure is very basic. It only consisted of infected nodes and C&C domains that used HTTP as its communication protocol.

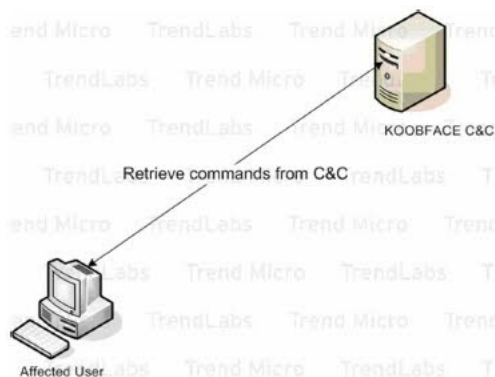


Figure 40. KOOBFACE C&C prior to July 19, 2009

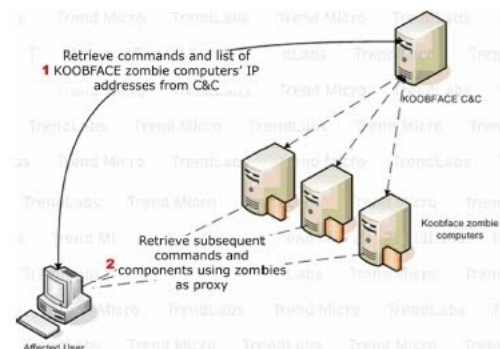


Figure 41. Updated KOOBFACE C&C as of July 19, 2009

This simplistic C&C approach is, of course, very vulnerable to takedowns. After several KOOBFACE C&C takedown attempts initiated by Internet service providers (ISPs) and members of the security industry,³ the KOOBFACE gang realized the need for a more robust C&C infrastructure. Thus, on July 19, 2009, the KOOBFACE writers implemented a new C&C architecture that involved the use of proxy nodes to provide redundancy and to improve the survivability of their C&C should another takedown be attempted.⁴

A few days after the new KOOBFACE C&C infrastructure was implemented, the botnet was seen inserting a message (see below) for one of the security researchers tracking the malware's domain activities.

```
(2009-07-22 20:24:17)
#We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com)
#for the help in bug fixing, researches and documentation for our software.
```

Cyber Intelligence by Dancho Danchev

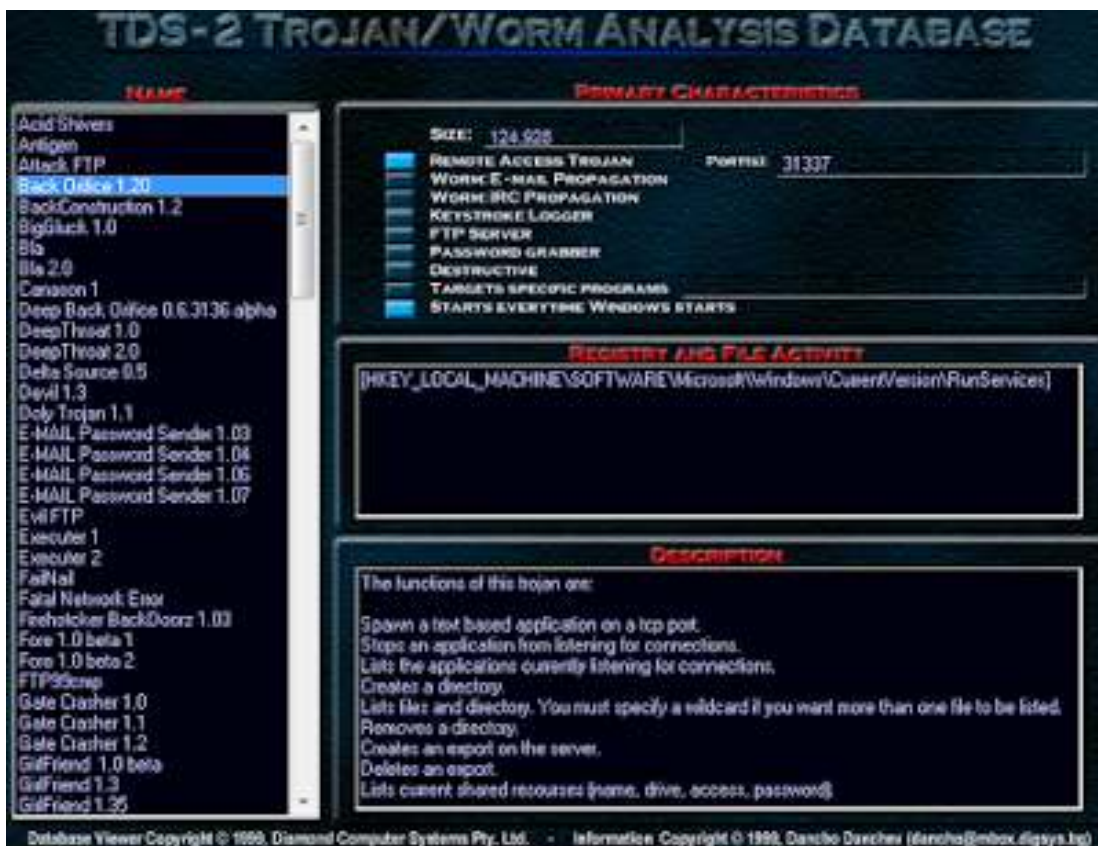
Back in 2011 while I was busy living in another town I actually met with a NYTime reporter for the purpose of catching up and elaborating more on my research on the Koobface botnet which was quite a success in terms of communicating my findings to a proper party which eventually led to a high-profile quote on my research on the Koobface botnet in the original NYTimes.com At a specific point in time my primary area of occupation included the active monitoring and taking down of the Koobface botnet which at the time was the only active social media propagating botnet that was successfully targeting Facebook in terms of spreading malicious software across the social media platform sucessfully affecting its users. The gang then continued its underground marketplace activities by starting to serve client-side exploits to users visiting major Koobface Web properties that also includes fake YouTube including Flash Player serving Web sites part of the Koobface botnet.

HNNCast052110



Cyber Intelligence by Dancho Danchev

During the 90's I had the privilege to own a personal computer among the few kids on the block that really had a personal PC at their place which at the time was an IBM clone known as Pravetz 16 which basically allowed me to explore the world of computers and technology while working with various files and actually spending most of my time playing computer games. I started getting involved in the world of hacking largely provoked by several movies such as for instance the original "Hackers" movie including the buzz around the very idea of compromising and penetrating another person or organization's PC seeking intellectual exploration as a basic motivation factor. Among my primary bookmarks at the time were <https://textfiles.com> including Box.sk and <https://astalavista.box.sk> including Progenic.com and naturally packetstormsecurity where I was busy going through the news on a daily basis potentially getting myself motivated by some of the latest web site defacements of high-profile Web sites around the globe.



Cyber Intelligence by Dancho Danchev

Among my first contributions in the field were several text files including the production of two issues of Trojan Defense Suite's Newsletter and the production of the security newsletter for Blackcode.com including several papers detailing the basics of trojan horses and how to use them including how to protect yourself against them including several text files in various categories including papers on anarchy. What I was particularly famous at the time with is the production of "The Complete Windows Trojans Paper" which at the time was the only and most popular text file explaining the basics of trojan horses and to protect yourself against them. Something else I was particularly popular with was my personal online hacking and security files repository which was actually featured on several top lists for hacking and security web sites including Progenic.com where I was getting a lot of traffic and there were actually quite a lot of people voting for my personal web site and supporting it. I was also specifically well known for producing several issues of the security newsletter for Blackcode.com which was a top and high-profile high-traffic visited portal for hacking resources back in the 90's where I had the privilege to produce the portal's security newsletter and contribute with actual articles on the topic.

```
--{ BlackCode Ravers Magazine Issue 2 }--  
Home page : http://www.blackcode.com  
Editor of the magazine: THE mAnIaC  
themaniac@blackcode.com
```

Table of Contents:

```
-----  
1.Editorial  
2.Mirrors of the magazine  
3.Latest News With BlackCode Ravers  
4.How to break your school security  
5.About virii  
6.Advertising  
7.Trojans section  
8.For the newbies  
9.Linux Section  
10.Interviews  
11.Final words  
-----
```

1. Editorial

```
=====
```

It's me again.This is our second issue.I've changed the design and I've added several new things in the newsletter. I've also received a lot of e-mails about our magazine. People like it and they want more information here. The first issue was short one but of course every new issue has many new things added in it. I'm happy people like it and we have MANY new subscribers every day. Also we have much more visitors than before.

Cyber Intelligence by Dancho Danchev

Quickly, entering, the, premises, of, the, doorway, Sten, yelled at, next door, neighbor, best, friend, and, both, quickly, left, the, premises, and, gathered, to, ask, for, more, of, his, friends, ready, to, go, to, school. Jesebelle, quickly, noticed, the, two, of, them, coming, their, way, and, carefully, prepared, to, go, to, school. On their way, they, met, Constantine, who, waited, for, them, to, gather, on, their, way, to, school.



Preparing, for, the, day, was, quite, a, gathering. Sten, entered, the, front, door, of, the, school, followed, by, Jezebelle and Constantine, and, his, best, friend, next, door, neighbor, Gater. Followed, by, the, most, of, the, students, back, there, the, class-mates, entered, the, classroom, and, sat, on, the, desk, table, ready, for, school. First, thing, Sten, did, was, to, prepare, for, class. He, unpacked, his, belongings, and, got, ready, thinking, about, what, he'll do, once, he, gets, back, home, sitting, in, front, of, his computer. The class, was, quite, a, gathering, with, all, of, his, classmates, entering, the, classroom, followed, by, their, friends, and, the, teacher. The class, began, followed, by, most, of, his, classmates, entering, the, room, with, the, teacher, slowly, checking, who's present, and, who's not. First, things, come, first, with, the, teacher, slowly, checking, who's, about, to, share, his, lesson.



First, thing, Sten, did, was, to, think, of, his, computer, back, home, a cozy, feeling, of, self-preservation, and ultimate, self-being, Sten, felt, the, power, of, his, loneliness, and, started, to, image, the, things, he'll, do, when, he, comes, back, home. The teacher, Mrs, Jozefine, quickly, realized, that, several, students, need, to, tell, their, lesson, and, started, asking, who's, decided, to, tell, their, lesson, first. Sten, quickly, decided, to, share, a, feeling, of, comfortability, with, his, next, desk, neighbor, and, quickly, smiled, thinking, about, all, the, things, he'll, do, when, he, gets, back, home. A, perfect, surrounding, and, a, room, full, of, personal, belongings, quickly, drove, Sten, to, realize, the, vast, potential, of, his, personal, mindset, allowing, him, to, consider, the, possibility, of, all, the, things, he'll, do, when, he, gets, back, home. His students, quickly, realized, that, the, time, to, tell, their, lesson, has, come, and, prepared, to, get, asked, by, their, teacher, about, everything, they, learned, about, their, lesson. First, things, come, first, with, several, of, his, classmates, getting, asked, about, their, teacher, and, what, they, learned, about, their, lesson.



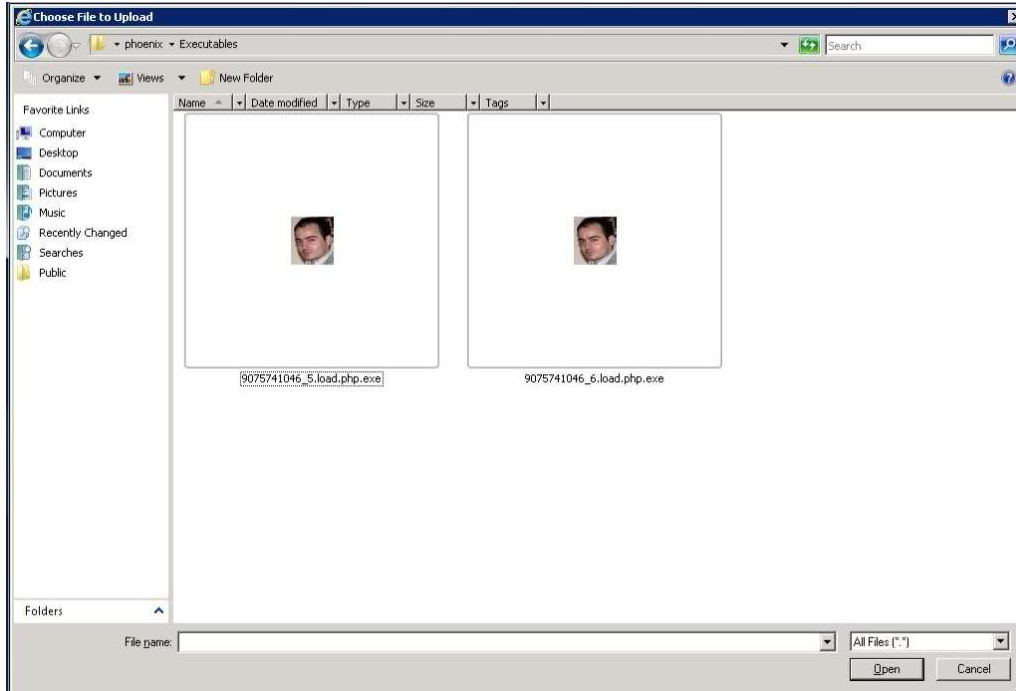
Sten, quickly, payed, attention, to, his, classmate, getting, asked, about, his, lesson, and, quickly, felt, the, comfortability, of, knowing, that, he, knew, his, lesson. Time, for, a, break, and, the, classmates, quickly, went, on, to, decide, on, how, to, change, rooms. While, the, room, was, changed, Sten, quickly, wandered, around, thinking, and, considering, the, possibility, of, owning, a personal computer, including, the, joys, and, benefits, of, sharing, his, belongings, with, someone, else. Next, lesson, comes, next, the, classmates, quickly, entered, a, new, room, and, started, getting, prepared, for, their, class.





The rush, through, the, hallway, quickly, embraced, Sten, and, his, friend, and, they, quickly, wandered, around, seeking, and, feeling, blissful, joys, of, shared, compatibility, with, the, surrounding, environment. Next, lesson, comes, next, and, the, friends, quickly, entered, a, new, room, quickly, busy, preparing, for, their, lesson. Unpacking, was, easy, a, textbook, a, notebook, a, pencil, and, various, related, materials, getting, ready, for, their, lesson. Sten, was, busy, considering, the, joys, of, owning, a, personal, computer, and, quickly, decided, that, thinking, about, it, made, him, feel, even, better. Considering, the, joys, of, owning, a, personal, computer, was, quite, an, experience, and, Sten, felt, even, better, while, considering, the, joys, and, a, feeling, of, belonging, to, a, personal, need, and, self-preservation, type, of, self-being, joyful, experience, allowing, him, to, further, expand, his, emotional, feeling, of, belonging, to, a, surrounding, environment, including, his, friend.

Cyber Intelligence by Dancho Danchev



With, lessons, about, to, get, over, Sten, and his, friend, decided, that, time, for, home, was, even, better, and, they, quickly, wandered, around, figuring, a way, to, find, the, hallway, as, they, decided, to, go, back, home. The trip, was, quite, a, pleasant, surprise, with, both, of, them, walking, the, same, path, as, they, walk, on, an occasional, basis, as, they, decided, that, time, for, home, was, even, better. Entering, the, hallway, was, quite, an, experience, and, both, of, them, feeling, a feeling, of, belonging, quickly, entered, the hallway, and, decided, that, time, for, home, was, even, better.

Quickly, packing, the, bags, was, easy, as, a lot, of, friends, decided, that, time, for, home, was, even, better, as, they, decided, that, time, for, home, was, even, better. Quickly, decided, that, time, for, home, was, even, better, Sten, and his, friend, quickly, packed, their, bags, and, went, on, to, see, their, friends, as, they, decided, that, time, for, home, was, even, better.

Cyber Intelligence by Dancho Danchev

Blog	% of covered IOCs	% of covered iocterns	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

Slowly entering the premises of what can be best described as home, grandma was quick to prepare lunch a cozy feeling of home-belonging and a warm fireplace feeling of personal self-belonging. While paying attention to what Sten managed to achieve during the day, grandma payed attention to his lesson by a personal feeling of belonging to what Sten would do next during the afternoon. Sitting and watching right behind him, grandma took the time and effort to pay attention to his lesson and a personal feeling of self-belonging quickly started to take place prompting Sten to learn his lesson even faster. The TV quickly ran a story following a placement of an animated cartoon aired on Ostankino a Russian national-TV back in the time called “Maya” the Bee.

Cyber Intelligence by Dancho Danchev

The time has come to play a game. Sten quickly powered his 16-bit Pravetz PC 2MB RAM and a screen full of computer game choices quickly appeared prompting him to choose a game. While loading a relatively known game known as Scorch Sten decided to play two hours and then proceed with meeting his friends and start a discussion with his grandma. A huge fan of strategy games Sten decided that he didn't have the time to dedicate to play his favorite game - Sid Meier's Civilization and instead he figured that he would eventually play the game later throughout the day. Playing Scorch was quite an experience and he took a few hours of his precious learning time to interact with the game. He then decided to approach his best friend at the time and co-conspirator in the World of UFO's the Soviet Union and computer games including the hacking Scene - George Kadiysky for two hours of extensive game play where we would strategize on how to best "approach" the Soviet Union in terms of invasion actively and carefully planning every move on our way to invade the Soviet Union and eventually all the surrounding countries. While I was busy preparing for our several hour game play

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

- **Kaspersky Lab** for the name of **Koobface** and 25 millionth malicious program award;
- **Dancho Danchev** (<http://ddanchev.blogspot.com>) who worked hard every day especially on our First Software & Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C&C) servers, and of course analyzing software under VM Ware;
- **Trend Micro** (<http://trendmicro.com>), especially personal thanks Jonell Baltazar, Joey Costoya, and Ryan Flores who had released a very cool document (with three parts!) describing all our mistakes we've ever made;
- **Cisco** for their 3rd place to our software in their annual "working groups awards";
- **Soren Siebert** with his great article;
- Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving **their** security system.

By the way, we did not have a cent using Twitter's traffic. But many security issues tell the world we did. They are wrong.

As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. **Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER.** As for the crashes... We are really sorry. We work on it :)

Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

George was supposed to be busy going through a CD which was basically a mirror of Packetstormsecurity in particular the E-Zine section so that we can prepare to have a conversation in terms of working out our technological and military strategy on our way to achieve global domination in the original Sid Meier's Civilization. What we basically did in the beginning was to strategize and actually get a better view of the technology tree of the game and while I was busy moving the Empire along George was busy keeping notes on our way to keep track and advance out military strategy on a "first come first serve" b

[Interacting with Koobface – a Case Study]



- Koobface Gang featured messages and greetings
 - C&C server communication featured messages and greetings - *"We express our high gratitude to Dancho Danchev (<http://ddanchev.blogspot.com>) for the help in bug fixing, researches and documentation for our software.*
- Multiple domains registered to typosquatted Dancho Danchev
 - pancho-2807.com is registered to Pancho Panchev
 - rdr20090924.info registered to Vancho Vanchev



6

asis.

25

7

Getting Connected

Cyber Intelligence by Dancho Danchev

Provoked by the need to reach out to a vast network of computers known as the Internet - Sten quickly decided that the time has come to get connected - so that he decided to seek a proper connection provider in his local hometown. Back in the day the primary connection providers in the time were Bulgaria's Digital Systems BIA Net and the country's leading mobile connectivity provider - Mtel's pre-paid dial-up cards. Times were different in terms of connectivity and DSL and ADSL were a dream come true in the face of corporate networks properly utilizing and using ISDN type of based connectivity. Keeping it simple - Sten decided to quickly acquire the necessary dial-up modem - which he would eventually fall in love with potentially reaching out to a vast network of computers known as the Internet using the help of a local dial-up provider known as Digital Systems. Back in the day - hourly based dial-up access meant think twice about what you do and how you do it online which means that I would have to basically prepare a plan for the things that I'll do online including Web sites which I would have to visit including a set of emails which I would have to send to a set of people including

friends and colleagues.





It's been years since he prepared to acquire a personal computer and get connected meaning that he managed to prepare a list of Web sites and newsgroups on the topic of hacking and computer security including general Web sites that he would eventually visit. Among the first Web sites that he visited was NBA.com where he would quickly learn about the latest developments on his favorite team including daily going through photos and possibly video material to showcase his favorite team at the time. Among the most venerable experienced he first discovered prior to getting connected is to search for UFO photos and information on the KGB including the active reproduction of sound using his

external speakers in a MIDI-dominated World at the time. The most venerable and unforgettable experience at the time was the fact that he had access to an email which he used to keep in touch with the Internet Service Provider's system administrator Bogdan Dochev so that he could keep in touch with him including the active sharing of new Web site links for him to visit and exchange communication.



Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.



Among the first groups which I really joined at the time was Toxic Crisco which basically represented a group of individuals involved in a variety of online activities including possibly hacking including the SCR Project which was basically a social engineering driven hacking group where I was proud to be a member of in particular my active involvement in reading various high-profile psychology books at the time.

For the purpose of using IRC in particular DALnet Stan quickly gathered a copy of the popular mIRC including several War Scripts ICQ Bombers Nukers and Mail Bombers including tro-jan horses and quickly decided that he should start getting experienced in the world of hacking for the purpose of gaining knowledge and impressing his friends. Among the first channels that he actually joined at the time were #gay and #lesbian where he was basically portraying himself as another person who was basically seeking to offer a new and novel photos-based screensaver to a variety of individuals for the purpose of tricking them into executing the screensaver on their home PCs ultimately gaining access to their PCs using a popular trojan horse client at the time such as for instance Sub7.

Cyber Intelligence by Dancho Danchev

On a beautiful Thursday afternoon Stan decided to play a decent computer game while his mother was busy ironing in the kid's room and decided to take a journey successfully getting the World rid of hostile aliens. The game called Duke Nukem basically took Stan on a journey to another World where he spend most of his afternoon getting rid of evil aliens while he led a discussion with his mother on his whereabouts during the day including active next-day class preparation and the eventual dinner conversation. While mom was busy ironing Stan took on another journey to a distant World where he took care of and protected the Earth from evil aliens and decided that the time has come for a rest.

Some of the most memorable memories of Sten back in the time have to do with playing full-time one of the best strategy games during the 90's that's Sid Meier's Civilization. Spending a decent portion of his time basically four hours on a daily basis Sten quickly acquired the necessary skills to take his civilization to a new level by waging wars developing and exchanging new technologies and by waging wars with competing and adversary civilizations.



Having already mastered the power of the Civilization game Sten quickly fell into a World of politics technologies and wars and successfully mapped and left a foothold in the World the way he knew and mastered having successfully spend a decent portion of his time playing the best strategy game during the 90's that's Sid Meier's Civilization. Game World is something different. Whenever Sten decided to play a game the World came to a halt with Sten playing and learning the basics and inner workings of every game that he managed to get his hands on throughout the 90's.

Pushing the boundaries of the game at some point Stan decided to take a deeper look at how you can actually make the com-puter's player become more advanced and sophisticated and actually tried to train the AI of the game and potentially figured out a way to teach to use advanced warfare tactics.



Cyber Intelligence by Dancho Danchev

The primary source of new games which were basically coming from Russian-distributed CDs at the time was Pavel Vitkov a close friend to Dancho who was actually possessing and was able to negotiate and obtain some of the latest and most popular games worth playing at the time. While Dancho was busy becoming a master of Sid Meier's Civilization most of his friends and colleagues at the time were busy playing another game part of the franchise known as Colonization which despite the fact that it was pretty similar to Sid Meier's Civilization couldn't really offer the necessary global politics and war strategy tactics including possible espionage tactics which Dancho was looking for in a modern game at the time.

It would be fairly easy to assume how things got complicated with Sten quickly obtaining access to Internet Relay Chat's primary mIRC application including a variety of IRC-based "War Scripts" including a dozen of mail-bombers and various other ICQ-based type of Nukers and Flooders on his way to demonstrate a proper technical know-how to his friends and peers in the shady world of hacking. Among the first channels he tried to access were #hacker #hackers #hacking and the infamous #hackphreak on EFNet including to actually open several personal channels on the local IRC networks including #drugs #KGB and #linuxsecurity. At a later stage he actually managed to ask a friend for a possible operator status on the local town's IRC channel where he was basically running a 24/7 online protection bot known as xexploit including the active use of a Socks5 server which at the time was offered by his employer LockDownCorp where he was busy acting as Technical Collector of trojan horses/worms/viruses and VBS scripts for the purpose of improving the anti-trojan software's signatures-based detection rates.

Cyber Intelligence by Dancho Danchev

Proxy Server Name	HTTP Port	SOCKS Port	Network #	Machine	IP BLOCK
BLACKCODEPROXY.COM	8080	1080	Network # 1	Machine # 1	216.41.20.82
TLPROXY.COM	8080	1080	Network # 2	Machine # 2	12.148.163.141
PROXY1.THEPROXYCONNECTION.COM	8080	1080	Network # 1	Machine # 3	216.41.20.120
PROXY2.THEPROXYCONNECTION.COM	8080	1080	Network # 1	Machine # 4	216.41.20.13
PROXY3.THEPROXYCONNECTION.COM	8080	1080	Network # 1	Machine # 5	216.41.20.37
HIDDEN-INPHERNO.NET	8080	1080	Network # 2	Machine # 6	199.105.112.152
DSL-NET.ORG	8080	1080	Network # 2	Machine # 7	63.127.192.136
ONTARIO-CA.NET	8080	1080	Network # 2	Machine # 8	199.105.112.163
GERMANY-DE.NET	8080	1080	Network # 2	Machine # 9	199.105.112.170
SHAWCABLE-CA.NET	8080	1080	Network # 2	Machine # 10	199.105.112.182
MODEM-LINK.NET	8080	1080	Network # 2	Machine # 11	199.105.112.186
CA-CABLE.NET	8080	1080	Network # 2	Machine # 12	63.127.192.178
INTERNET-PIPELINE.NET	8080	1080	Network # 2	Machine # 13	199.105.112.190
WIRELESS-INET.NET	8080	1080	Network # 1	Machine # 14	216.41.20.175
STAR-TRAVEL.ORG	8080	1080	Network # 1	Machine # 15	216.41.21.20
POPULAR-PEOPLE.ORG	8080	1080	Network # 2	Machine # 16	12.148.163.51

Sample Socks5 Commercially-available servers courtesy of LockDownCorp one of Stan's current employers at the time which he used to increase his reputation on the local IRC Network and to actually hide his real IP

Among the first thing that Stan decided to do in his spare time is to actively research the local Webmaster of his hometown's official Web site for the purpose of attempting to launch a social engineering attack against his local town's official Web site which basically succeed and resulted in a "greeting" message being posted on the official Web site with no actual data destruction and data removal taking place in what would appear to be a professional approach when compromising a legitimate Web site for the purpose of greeting his personal friends and spread a message on behalf of "Trojan Hacking Group" which at the time basically consisted of one of his closest friends and another fellow hacker enthusiast.



Sample Web Site Defacement courtesy of Stan throughout the 90's which basically resulted in a personal message and a personal greeting to all of his friends at the time courtesy of "Trojan Hacking Group"

Among his responsibilities the time included the active collection of trojan horses/worms/viruses and VBS Scripts with the idea to share them with his employer which at the time was LockDownCorp one of the world's leading anti-trojan vendors for the purpose of improving the detection rate for these publicly accessible trojan horses in what would later on mature into a successful Technical Collection operation which basically paid his bills and actually offered him a decent financial incentive to continue getting involved in security as a hacker enthusiast and actually improved his employer's overall detection rate for some of the most prolific trojan horses at the time.

The actual contractual agreement had to do with Stan using a private FTP server where he would spend hours uploading collected trojan horses using his home-based dial-up connection and eventually earning a revenue in the process using Western Union where he was happy to have established direct working relationship with one of the world's leading anti-trojans vendors which at the time was located at -
<http://proxy2.stealthedip.com/maniac/incoming/>

Cyber Intelligence by Dancho Danchev

	Parent Directory	17-Apr-2002 13:06	-
	Cyn1.2.zip	05-Dec-2001 15:44	124k
	Fr1.55lite.zip	05-Dec-2001 15:55	207k
	Fr1.56lite.zip	05-Dec-2001 15:56	50k
	Gift2.1.1.zip	05-Dec-2001 16:02	314k
	Homeunix1.0.zip	05-Dec-2001 16:04	224k
	HoneyPot1.1.zip	05-Dec-2001 16:08	185k
	MantisBeta2.zip	05-Dec-2001 16:09	128k
	Metal2.7.zip	05-Dec-2001 16:11	211k
	Olive2.4.zip	05-Dec-2001 16:25	145k
	OptixGW.zip	05-Dec-2001 16:25	35k
	Psychofiles1.8.zip	05-Dec-2001 16:28	623k
	fatalconnection20.rar	05-Dec-2001 16:00	734k
	input.rar	05-Dec-2001 16:09	2k
	nerte722.rar	05-Dec-2001 16:15	798k
	nerte733.rar	05-Dec-2001 16:23	798k
	nerte74.rar	05-Dec-2001 16:57	1.1M
	nerte75.rar	05-Dec-2001 17:12	1.1M
	[] ptakks21.exe	05-Dec-2001 16:31	455k
	rembomb.rar	05-Dec-2001 16:32	10k
	revengor.rar	05-Dec-2001 16:36	192k
	rnsfire.zip	05-Dec-2001 16:36	11k
	rnstick.zip	05-Dec-2001 16:37	131k
	rnsuploadtrojan.zip	05-Dec-2001 16:38	11k
	skyrat.rar	05-Dec-2001 16:44	362k

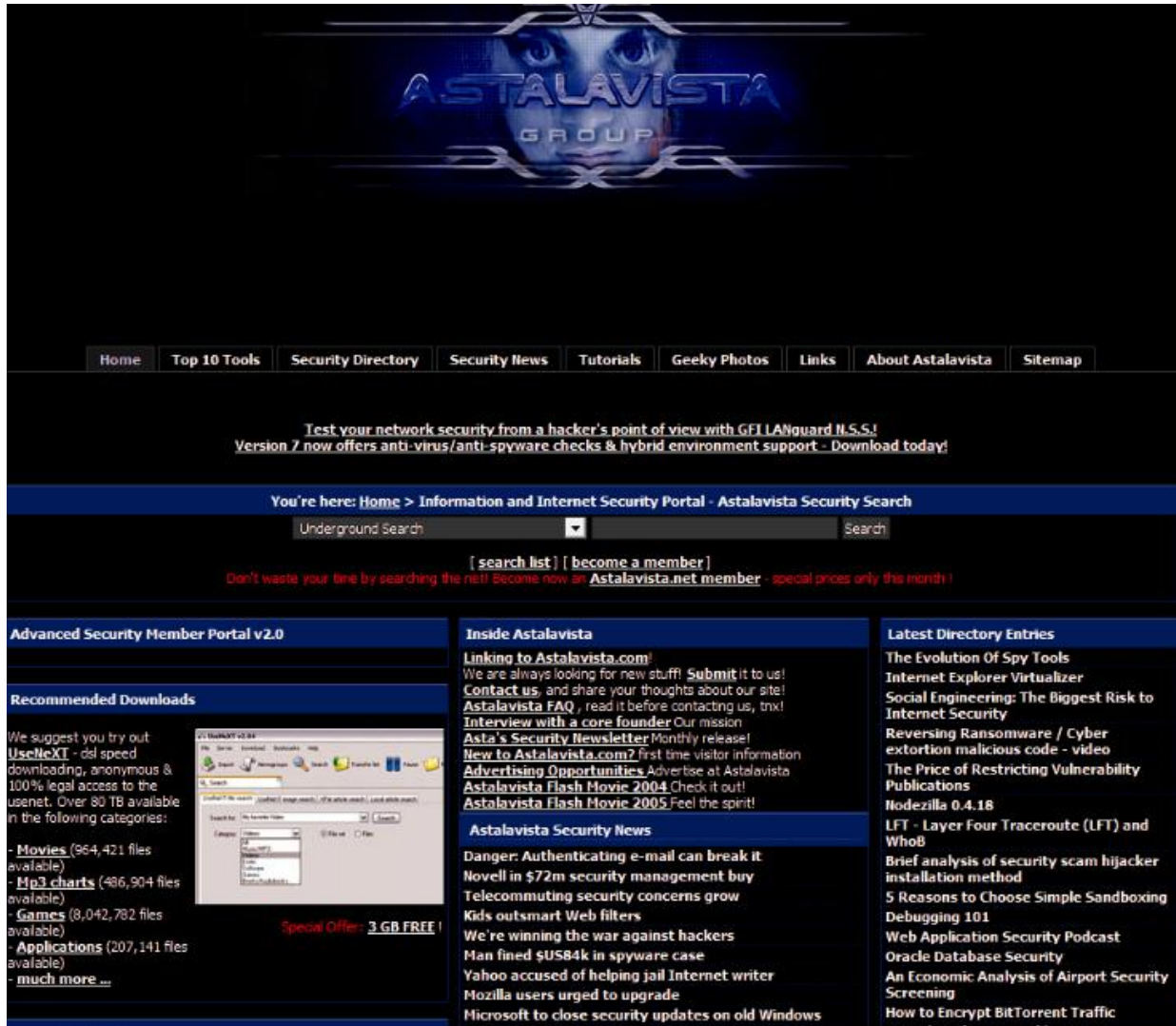
Sample Directory Listing of Stan's personal directory at oxy2.stealthedip.com/maniac/incoming/ LockDownCorp's FTP server where he was busy collecting and sharing trojan horses/worms/viruses and VBS Scripts and actually earning revenue in the process

Whenever Stan would attempt to reach out to his friends he would attempt to find out whether they are online using a popular trojan horse including to actually check his email account for their recently changed passwords and other related information including their current IP so that he can properly connect to their home PC for educational purposes.



The primary purpose for connecting to a friend's PC using a popular trojan horse would be purely for educational purposes with no actual hard or any sort of eavesdropping taking place.

While Dancho was busy studying in the Netherlands he was busy persistently checking one of the World's most popular and high-trafficked Web sites for hackers and security experts Astalavista.com - and sticking to the common wisdom circa the 90's where everyone was busy making contributions and launching new groups - he decided to approach the company behind the portal with a possible business proposal that basically consisted of having him monitor and actually maintain the portal in terms of content including the actual production of a high-profile Security Newsletter where we would produce security and hacking articles including a featured Security Interview with key members from the Scene and the Security Industry.








Sample Screenshot of the Astalavista.com Information Security Portal which Dancho Danchev was running as a Managing Director 2003-2006 where he was basically responsible for all the content

Prior to getting a confirmation from a Team Member of the actual owner of the portal at the time Dancho quickly began entering into negotiations about a possibly paid including a free venture at the time where he could earn a small comission for producing a high-quality security newsletter and actually be responsible for all the security and hacking content at Astalav-ista.com on a monthly and daily basis.

Cyber Intelligence by Dancho Danchev

Mitarbeiter der Astalavista Group

	Ivan Schmid - Dipl. Ing. FH Telecom Mitglied der Geschäftsleitung Leitung Entwicklung, Security Engineer		Pascal Mitter - Dipl. Ing. FH Telecom Mitglied der Geschäftsleitung Leitung Produktmanagement, Security Engineer
	Christian Wehrli - Dipl. Ing. FH Telecom IT Application, Security Engineer		Thomas Kälin - Lehrling Entwicklung, Support
	Paulo Santos - Praktikant Advanced Security Member Portal, Support		Melanie Bossert - Lehrtochter Entwicklung, Support

Frei/externe Mitarbeiter

Joe Madrecki (England) Selbstständig Webmaster/Redaktor	Dancho Danchev (Bulgaria) Managing Director, Astalavista.com	Fabrice Kjaerdt (Dänemark) Architekt FH/Design (IA) Webmaster/Entwicklung
--	--	--


Sample Screenshot of Astalavista.ch's About Us Section where Dancho Danchev used to work during his student years in the Netherlands as a Managing Director at Astalavista.com

As he began working on the monthly newsletter the first issue including the remaining twenty six issues which he produced over a period of three years were quite a success including the actual Geeky Photos section where portal users could send in photos of their desktop computers for the purpose of featuring them at the Web site potentially promoting their desktop setups to our audience at the time eventually leading him and the portal to win a PCMagazine Top 100 Security Sites Award back in 2005.

Astalavista Security Group
04.06.05
Discuss **Total posts: 1**

www.astalavista.com

Google pages indexed: < 100,000
Backlinks: < 1,000,000

 Started by a hacker/enthusiast in 1997, Astalavista has grown into an amazing melting pot of black hats, white hats, and everything in between. Whether you're learning how to be digitally naughty or you want to know how to avoid becoming a victim, it's hard to find a better mixture of battlefront news, tips, cracks, and hacks.

<< **MAIN**

next >

Print Email Save Rate it Reprints

Sample screenshot of Dancho Danchev's Astalavista.com Winning a PCMagazine.com Top 100 Security Sites Award for 2005

Among Dancho's main responsibilities at the time where the daily updating of the portal with high quality security documents tools and presentations including actual hacking and security links and overall responsibility for all the content at the Web site including the production of a highly popular security newsletter at the time including to actually answer and work on possible partnership and advertising inquiries at the time which led to a successful repositioning of the portal as one of the primary information security portal services online.

Among the key folks and individuals that he interviewed during his management of Astalavista.com and asked some pretty decent and relevant questions at the time include:

Cyber Intelligence by Dancho Danchev

- Proge, Progenic.com
- Jason Scott, TextFiles.com
- Kevin Townsend, ITSecurity.com
- Richard Menta, BankInfoSecurity.com
- Mr. Yowler, Cyberarmy.net
- Prozac, Astalavista.com
- Candid Wuest, Security Researcher
- Anthony Aykut from Frame4.com
- Dave Wreski from LinuxSecurity.com
- Mitchell Rowton from SecurityDocs.com
- SnakeByte from Snake-Basket.de
- Björn Andreasson from WarIndustries.com
- Bruce from DallasCon.com
- Nikolay Nedyalkov from ISECA.org
- Roman Polesek from Hakin9.org
- John Young from Cryptome.org
- Eric Goldman EricGoldman.org
- Robert, CGISecurity.com
- Johannes B. Ullrich, CTO of the Sans Internet Storm Center, and the main developer behind the Dshield.org project
- Daniel Brandt, Google-Watch.org
- David Endler, TippingPoint.com
- Vladimir, 3APA3A, Security.nnov.ru
- Johnny Long, johnny.ihackstuff.com
- Martin Herfurt, Trifinite.org



Personal Photo of Dancho Danchev Presenting at CyberCamp 2016 on "Exposing Koobface - The World's Largest Botnet"

Being the World's most notable cybercrime researcher security blogger and threat intelligence analyst the researcher quickly gained fame by systematically and efficiently profiling and analyzing a decent snapshot of malicious nation-state and fraudulent activity online leading him to pursue a successful career as the World's most popular cybercrime researcher security blogger and threat intelligence analyst.

In an early Monday morning the researcher quickly gathered a set of research materials of the primary botnet that's he's been monitoring the infamous Koobface botnet using passive and active virtual SIGINT methodologies which basically include active sampling of the botnet's malicious online activities using a daily set of intercepted malicious and fraudulent campaigns launched managed and operated by the Koobface botnet for the purpose of providing the necessary technical operational and strategic OSINT type of intelligence including the daily batch of money mule recruitment domains and campaigns which he was busy profiling with the idea to assist U.S Law Enforcement on its way to track down and prosecute the cybercriminals behind these campaigns.

Cyber Intelligence by Dancho Danchev

The screenshot displays a YouTube video player for a video titled "Sexy Hidden Camera". The video content is a red-tinted window titled "ADOBE FLASH PLAYER" with a white text box. The text inside the box reads: "An update to your Adobe Flash Player is available. Flash Player enhances your Web browsing experience. This update includes: Full screen, HD video playback; Cinematic special effects that bring Web experiences to life; Faster performance." Below this text are buttons for "Install Now", "Remind Me Later", and "Don't Install".

Below the video player, the video's metadata is shown: 137 ratings (represented by stars), 482,245 views, and options for Favorite, Share, Playlists, and Flag. The share options include MySpace, Facebook, and Twitter. There are also sections for Video Responses (0) and Text Comments (33).

The comments section shows several user interactions:

- jordanone38** (2 weeks ago): "hmmm i like that one... its familiar to the video i watch in webstree43(dot)tk..... hope you can watch it too LOL"
- jeridas** (3 weeks ago): "jussaaaaaaaaaaaaa"
- filajah** (1 month ago): "kako ove balerine vole da vide kitu i ne skidaju pogled ich"
- poormansvideo** (1 month ago): "that*"
- poormansvideo** (1 month ago): "they where not scared. the means they want that cock! :P"

The right sidebar features a "More From: 7770robi" section and a "Related Videos" section with thumbnails and titles such as "Hidden camera- rebel miniskirt", "Sunbed babe, Hidden camera", "skritta kamera", "Skrivena Kamera stikla", "Hidden camera- big dick", and "Sexy Hidden Camera Bath Prank (LOL)".

The Koobface botnet was the primary botnet propagating over social media at the time in particular Facebook and has already managed to affect tens of thousands of users globally potentially enticing them to interact with rogue and visual social engineer-ing based type of malicious and fraudulent campaigns in the form of Fake Adobe Flash Players and fake YouTube videos where the ultimate goal would be to attempt to affect their friends on Facebook by sending automated and legitimately looking messages including links to rogue and malicious content.

What what particularly interesting about the Koobface botnet at the time was the easy to track down and monitor actual C&C and campaign infrastructure where I was busy tracking it down and publishing my findings on a daily basis for the purpose of empowering my blog readers and the security community

Cyber Intelligence by Dancho Danchev

with the necessary threat intelligence on the actual whereabouts of the Koobface botnet in terms of offering as much technical details as possible with the idea to profile and keep track of its campaigns potentially assisting Facebook at the time including fellow security researchers on their way to track down and monitor the campaign.

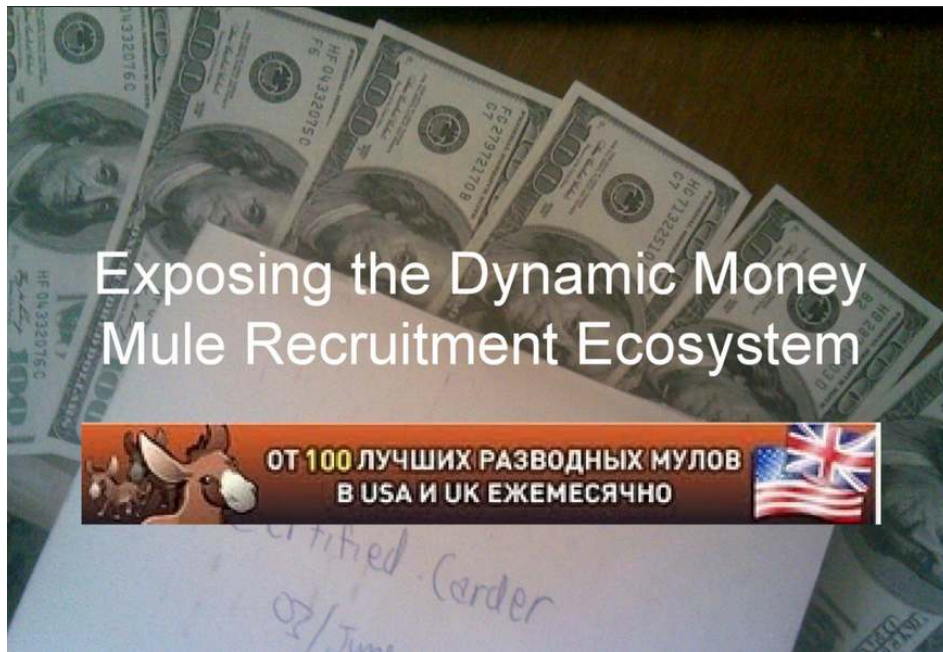
Bonus Content - Visiting GCHQ

Back in 2008 I got the personal privilege to attend a high-profile conference event organized by the HoneyNet Project at the GCHQ where I got a personal invitation to attend the event and make a presentation on the topic of cybercrime research which I did and actually attended the event where I had the privilege and honor to meet some of the key people behind the HoneyNet Project where we exchange ideas and I had the privilege to make a high-profile presentation which is entitled "Intell on the Criminal Underground - Who's Who in Cybercrime for 2007".



Bonus Content - Interpol Conference

In 2010 I've received a direct invitation to attend one of the industry's leading invite-only cybercrime fighting conference which at the time was held at an undisclosed location where I had the privilege to held a high-profile presentation on money mule recruitment technique and practices including to actually meet and hang out with some of my friends and colleagues from the security industry which was quite a privilege and an honor.



Bonus Content - RSA Europe 2012

Back in 2008 I got the personal privilege to attend a high-profile conference event organized by the HoneyNet Project at the GCHQ where I got a personal invitation to attend the event and make a presentation on the topic of cybercrime research which I did and actually attended the event where I had the privilege and honor to meet some of the key people behind the HoneyNet Project where we exchange ideas and I had the privilege to make a high-profile presentation.



Bonus Content - CyberCamp 2016

Back in 2008 I got the personal privilege to attend a high-profile conference event organized by the Honeynet Project at the GCHQ where I got a personal invitation to attend the event and make a presentation on the topic of cybercrime research which I did and actually attended the event where I had the privilege and honor to meet some of the key people behind the Honeynet Project where we exchange ideas and I had the privilege to make a high-profile presentation.



Bonus Content - InfoSec 2012

Back in 2008 I got the personal privilege to attend a high-profile conference event organized by the HoneyNet Project at the GCHQ where I got a personal invitation to attend the event and make a presentation on the topic of cybercrime research which I did and actually attended the event where I had the privilege and honor to meet some of the key people behind the HoneyNet Project where we exchange ideas and I had the privilege to make a high-profile presentation.

