Bil Oleg Viktorovich
Male, 38 years old, born June 15, 1982

newsoft2003@mail.ru

Residence: Nur-Sultan
Citizenship: Kazakhstan, has a work permit: Russia, Kazakhstan
Ready to move: Russia, Kazakhstan, ready for business trips

Desired position and salary

Information security, virus analyst, security consultant, programmer

Information technologies, internet, telecom

- Programming, Development
- Computer security
- CIO, IT Director

Employment: full time
Working hours: full day

Desired travel time to w ork: Doesn't matter

Work experience —16 years 6 months

March 2017 -
present
3 years 7 months

RSE "State Technical Service"

Nur-Sultan, w ww.sts.kz

Chief Architect - Head of the Malicious Code Research Laboratory

Chief architect - from March 2017, head of the laboratory - from November 2017.

Reverse of malicious softw are (x86, x64) (WinDbg, IDA, Hiew , Olly Debugger), detection and neutralization of malw are, investigation of incidents related to the impact of viruses;
Analysis of shellcode and exploits contained in infected files in office formats: PDF, RTF, SWF, OLE2 (*.doc, *.xls, *.ppt), *.docx, *.xlsx, *.pptx;
Parsing malicious scripts (AutoIt (au3 / a3x), JavaScript, VBScript, bat and macro viruses (MS Word, MS Excel)).
Deobfuscation, decryption of obfuscated or encrypted objects (executable modules, config files, malw are logs).
Research of components of targeted attacks, description of the communication protocol (list and format of commands) of malw are w ith C&C servers.
Analysis of RAM dumps, disk images in order to detect malw are.
Teaching a course on malw are analysis and delivering selected lectures on combating malw are: L. N. Gumilyov Eurasian National University, State Institution "Center for training and advanced training of specialists in the field of information security" of the Prime Minister’s Office of the Republic of Kazakhstan.
Became one of the w inners of the crackmy analysis competition held by JSC Kaspersky Lab (2016).
Prepared 2 papers for speaking at the Positive Hack Days conference (2017): Askar Dyusekeyev - Ransomw are Analyzer (consultant) and Anastassia Parygina (L.N. Gumilyov Eurasian National University) - “Development of an extension for the Google Chrome brow ser that protects against leakage of confidential textual information through other extensions "(supervisor of this thesis).
Made presentations at conferences BIS Summit (2018, Baku, Azerbaijan), Positive Hack Days (PHDays) (2018, Moscow), SOC-Forum Kazakhstan (2017, 2018, Astana), SOC-day Kazakhstan

(2019, Nur-Sultan), Security Analyst Summit 2019 (sas.kaspersky.com, Singapore).

Gave an interview to anti-malware portal anti-malware.ru
Details and links - in the "About me" section.

September 2015 - March 2017

1 year 7 months

KZ-CERT, a subdivision of the RSE "State Technical Service"

Nur-Sultan, kz-cert.kz/ru/

Chief Specialist for Malware Analysis (Virus Analyst)

Reverse of malicious software (x86, x64) (WinDbg, IDA, Hiew, Olly Debugger), detection and neutralization of malware, investigation of incidents related to the impact of viruses;
Analysis of shellcode and exploits contained in infected files in office formats: PDF, RTF, SWF, OLE2 (*.doc, *.xls, *.ppt);

Parsing malicious scripts (AutoIt (au3 / a3x), JavaScript, VBScript, bat and macro viruses (MS Word, MS Excel)).

Deobfuscation, decryption of obfuscated or encrypted objects (executable modules, config files, malware logs).

Research of components of targeted attacks, description of the communication protocol (list and format of commands) of malware with C&C servers.
Analysis of RAM dumps, disk images in order to detect malware.

Teaching a course on malware analysis and delivering selected lectures on combating malware: L. N. Gumilyov Eurasian National University, State Institution "Center for training and advanced training of specialists in the field of information security" of the Prime Minister’s Office of the Republic of Kazakhstan.

Became one of the winners of the crackmy analysis competition held by JSC Kaspersky Lab (2016).

September 2004 - August 2015

11 years

A. Baitursynov Kostanay State University

Kostanay, www.ksu.edu.kz

Head of the Software Development and Implementation Sector, Administrator for the Implementation of New Technologies, Acting administrator for the introduction of new technologies

Reverse of malicious software (x86, x64) (WinDbg, IDA, Hiew, Olly Debugger), detection and neutralization of malware, investigation of incidents related to the impact of viruses;
Analysis of shellcode and exploits contained in infected files in office formats: PDF, RTF, SWF, OLE2 (*.doc, *.xls, *.ppt);

Parsing malicious scripts (AutoIt (au3 / a3x), JavaScript, VBScript, bat and macro viruses (MS Word, MS Excel)), deobfuscation (decryption) of obfuscated or encrypted objects;
Development of a course on malware analysis: detection and neutralization (without using antivirus software), as well as static and dynamic analysis of malware. The course was delivered during the spring 2015 semester. Feedback from students and colleagues is positive.
Preparing students for participation in the student scientific conference "IT-Security for the Next Generation" held by JSC Kaspersky Lab, management of the student anti-virus laboratory, in cooperation with JSC Kaspersky Lab

Direct development of software, analysis of data obtained with its help, research of the current state of information technology, analysis of ways of development of information systems of the university, development of proposals to improve the efficiency of using computer technology, management of the software development and implementation sector (3 developers), configuration and maintenance Kaspersky Security Center servers (Administration Kit) (monitoring and managing anti-virus software - a network of about 1000 computers), performing information security work (dealing with incidents related to attacks on the website, etc.), preventing such incidents.
Technical support of the process of recruiting applicants at KSU.

April 2004 - August 2015

National Testing Center, RGSE

Nur-Sultan, www.testcenter.kz

11 years 5 months

engineer-programmer

Organization and implementation of various testing procedures (UNT, CTA ...) in the branch of Kostanay, also performed special work (confidential information), with a visit to Astana, from 2008 to 2015.

October 2010 - May 2012

JSC Kaspersky Lab, A. Baitursynov Kostanay State University

Kostanay, www.kaspersky.ru

1 year 8 months

coordinator of the student laboratory, jointly with JSC "Kaspersky Lab"

Prepared students for three conferences "IT-Security for the Next Generation" held by JSC "Kaspersky Lab", in 2010, work "Social Engineering", student Tuyakbaev Arman, 3rd place in Moscow, M.V. Lomonosov Moscow State University (Russia and CIS tour of the named conference), participation in the International tour, Jagiellonian University, Krakow, Poland; in 2011, students Vladimir Berdnik and Maxim Tsvetkov, work "A system for detecting unknown malicious programs in a corporate network for the analysis of suspicious activities", second place in Moscow, M.V. Lomonosov Moscow State University, participation in the International Tour, Munich Technical University, Munich, Germany; in 2012, student Maxim Tsvetkov, work "Development of a system for preventing information leaks during targeted attacks in corporate networks", was among the winners of the conference's correspondence round, participation in the face-to-face tour, E. Bauman MSTU, Moscow.

September 2011 - January 2012

JSC NWF Samruk-Kazyna

www.sk.kz

5 months

finalist of the competition

was among the finalists (21 people in various fields) of the republican competition "Innovative Kazakhstan", organized by JSC NWF Samruk-Kazyna - a fund that manages state-owned stakes in various companies, the main goal of which is the modernization and diversification of the national economy (www.sk.kz). The total number of participants in the competition was over 2,300.

July 2004 - September 2004

A. Baitursynov Kostanay State University

Kostanay, www.ksu.edu.kz

3 months

Information Analytical Center Engineer

Software development

Education

Higher

2004

A. Baitursynov Kostanay State University, Kostanay

Information systems in economics, economist-informatics with knowledge of English

Advanced training, courses

2019

Remote Forensics for the Modern Malware Hunter

Kaspersky Lab, Course held as part of the Information Security Summit (Security Analyst Summit)

2018

The God-Mode - practical training in static analysis of malware used in targeted attacks

Kaspersky Lab, Course held as part of the Information Security Summit (Security Analyst Summit)

2017

Malware analysis (Malware Reverse Engineering)

Kaspersky Lab, Course held as part of the Information Security Summit (Security Analyst Summit)

2014

Building an Information Risk Management Toolkit - remotely

University of Washington (via coursera.org)

2014

Designing and Executing Information Security Strategies - remotely

University of Washington (via coursera.org)

2014

Information Security and Risk Management in Context - remotely

University of Washington (via coursera.org)

2014

Usable Security - remotely

University of Maryland, College Park (via coursera.org)

2013

Malicious Software and its Underground Economy: Two Sides to Every Story - remotely

University of London (via coursera.org)

2011

Effective manager course

Center for Practical Psychology at A. Baitursynov KSU, Certificate

2010

Cryptographic information protection systems

State Institution "Center for training and advanced training of specialists in the field of information security" of the Prime Minister’s Office of the Republic of Kazakhstan, Certificate

2006

Information Security. Development of an information security policy.

State Institution "Center for training and advanced training of specialists in the field of information security" of the Prime Minister’s Office of the Republic of Kazakhstan, Certificate

Key skills

Languages

Russian — Native
English — C1 — Advanced
Kazakh — B2 — Upper intermediate
German — A1 — Beginner

Skills

Malware analysis Information Security Information Technologies Programming Providing anti-virus protection IDA Olly Debugger Virus research Analytical researches Assembler

Additional Information

Recommendations

LLP Information Technologies 5 plus
B. Abdikasov (General Director)

About me

Analysis of malicious software (WinDbg, IDA, Hiew, Olly Debugger), detection and neutralization of malware, investigation of incidents related to the impact of viruses;
analysis of shellcode and exploits contained in infected files in office formats: PDF, RTF, SWF, OLE2 (*.doc, *.xls, *.ppt);

analysis of malicious scripts (JavaScript, VBScript, bat and macro viruses (MS Word, MS Excel)), deobfuscation (decryption) of obfuscated or encrypted objects;

specialized software for analyzing and fighting viruses: Sysinternals: TCPView, RegMon, FileMon, RegShot, ProcessExplorer, DebugView; Wireshark, ImpREC, DeDe (Delphi decompiler), AVZ, HiJackThis, GMER, RootkitUnhooker, HIEW, WinHEX, Malzilla (malware analyzer), Volatility, Kaspersky Rescue Disk, Kaspersky Virus Removal Tool, Kaspersky Security Center (Administration Kit), antiviruses, firewalls, etc.;

computer investigations: ProDiscover, The Sleuth Kit, Autopsy;

data recovery: Ontrack Easy Recovery, PC Inspector File Recovery;

cryptography: PGP, TrueCrypt;

programming in languages and programming environments: Delphi, PHP, Visual C, VBA (Excel, Word), VBScript, JScript, Assembler (code analysis), DDK (development of kernel mode drivers for MS Windows), WinAPI;

work with database management systems (DBMS): MS SQL, MySQL, Oracle, work with heterogeneous data sources (combining data from several sources, under the control of different DBMS (via ODBC, ADO));

information security: analysis of information security risks, creation of a strategy for protecting data processed by specialized software against various types of attacks;

Virtualization software (VMWare);

MS Office (Excel, Word, Access, PowerPoint, FrontPage, Outlook);

graphic editor (Adobe Photoshop - user);

working with various programs of state bodies (tax, statistical, etc.), writing non-standard procedures for exporting / importing data from these programs, including parsing their data storage formats;

Prepared students for three conferences "IT-Security for the Next Generation" held by JSC "Kaspersky Lab", in 2010, work "Social Engineering", student Tuyakbaev Arman, 3rd place in Moscow, M.V. Lomonosov Moscow State University (Russia and CIS tour of the named conference), participation in the International tour, Jagiellonian University, Krakow, Poland; in 2011, students Vladimir Berdnik and Maxim Tsvetkov, work "A system for detecting unknown malicious programs in a corporate network for the analysis of suspicious activities", second place in Moscow, M.V. Lomonosov Moscow State University, participation in the International Tour, Munich Technical University, Munich, Germany; in 2012, student Maxim Tsvetkov, work "Development of a system for preventing information leaks during targeted attacks in corporate networks", was among the winners of the conference's correspondence round, participation in the face-to-face tour, E. Bauman MSTU, Moscow.

Advised Askar Dyusekeev's project on countering ransomware (ransomware) Trojans, which was presented at the Talent Lab competition held by JSC Kaspersky Lab (March 2017, Moscow). The result - a special prize - a trip to the conference on information security "Positive Hack Days" (https://academy.kaspersky.com/talentlab/international-final/). Askar also went through the work that I consulted, selection and spoke at the conference on information security Positive Hack Days 2017 (http://2017.phdays.ru/press/news/241925/).

Supervised the graduation work of Anastasia Parygina "Development of an extension for Google Chrome that protects against information leakage through other extensions."

Result: the work was accepted as a report in the Young School section of the conference on information security Positive Hack Days 2017.

Description: https://www.phdays.ru/program/246235/

Presentation: https://www.slideshare.net/phdays/google-chrome-76514783

Participated in the Security Analyst Summit held by Kaspersky Lab (March-April 2017, Saint-Martin, March 2018, Cancun, Mexico, April 2019, Singapore). Within the framework of these summits, took the following courses:

1. Malware Analysis (Malware Reverse Engineering) (2017). Lecturer - Nicolas Brulez - Principal Security Researcher of Kaspersky Lab.

2. The God-Mode Practical Training in Static Analysis of APT Malware (2018) - Igor Sumenkov and Sergey Golovanov are leading anti-virus experts at Kaspersky Lab.

3. Remote Forensics for the Modern Malware Hunter (2019) - Vitaly Kamluk - Leading Expert of Kaspersky Lab, Nicolas Collery - Head of the Red Team at DBS Bank.

Participated in conferences as a speaker:

1. Positive Hack Days (PHDays) (Moscow, 2018).

Presentation: https://static.ptsecurity.com/phdays/presentations/viruses-in-kazakhstan.pdf

2. BIS Summit held by the company InfoWatch (Baku, Azerbaijan 2018).

3. Security Analyst Summit, Kaspersky Lab, sas.kaspersky.com (Singapore, 2019) - report on

targeted attacks in Kazakhstan.
Also took part at a large number of conferences in Kazakhstan.
Gave an interview to anti-malware portal anti-malware.ru: https://www.anti-malware.ru/interviews/2018-07-19/26879
Security Analyst Summit 2019 (sas.kaspersky.com, Singapore)