

867 Lewis Ave,
Sunnyvale, CA
94086

Phone: (408) 203-4323
nbilogorskiy@gmail.com

<http://www.nickolay.ca>
<http://www.linkedin.com/in/bilogorskiy>

Nick Bilogorskiy

8 years in the computer security industry, specializing in reverse engineering malware, incident response, security team building and botnet takedown

Experience

March 2010 – May 2011 **Facebook** Palo Alto, CA

Lead malware researcher

- Investigate and track botnets and work with law enforcement agencies
- Coordinate and develop effective tools to detect malware
- Provide response to security incidents, code security audits, cyber crime investigations
- As malware subject matter expert, advise the engineering team on security requirements
- Engaged in building a world class malware response function

June 2006 – March 2010 **SonicWALL** Sunnyvale, CA

Manager, Malware Research

- Malware and vulnerability analysis, virus trends, quoted in the media
- Built and managed a team of world-class researchers
- Developed patent-pending “cloud antivirus” technology

Feb. 2004 – May 2006 **Fortinet Technologies** Burnaby, BC

Manager, Malware Research & Escalation

- Directed a team of international researchers from the USA, Canada, France, and China
- Increased the coverage of Fortinet in the media, improved quality of detection and descriptions
- Built a QA team and developed a testing process to test the Antivirus Engine

Jan. – Dec. 2003 **Art In Motion** Coquitlam, BC

Programmer / Analyst

- Developed customized solutions for the Licensing Department [XML, VB, SQL, Outlook API]

Jan. – May 2002 **Microsoft Corporation** Redmond, WA

Software Test Engineer - Intern

- Feature testing for MS Word. Made specs, test plans and automation [Word API, VB, XML]

2000 – 2001 **Randronics Digital** Burnaby, Canada

Founder / Lead web designer

- Founded a web design company and built several commercial websites [SQL, Flash, DHTML]

Education

2000–2003 **Simon Fraser University** Burnaby, Canada

- Bachelor of Science, Computing Science; Concentration: Software Engineering, AI, Philosophy

Projects

Facebook: Koobface botnet takedown

March 2011

For two years the Koobface worm was spreading on Facebook, infecting millions of Windows users who clicked on a malicious link in an infected friend's message. I worked on the attribution and enforcement on Koobface authors and the coordination of Koobface assets takedown. In March 2011 the efforts paid off when Koobface stopped targeting Facebook.

Facebook: Anti-Clickjacking measures

February 2011

After its launch, Facebook's LIKE feature was widely abused by rogue affiliate scams (likejackers). I helped build a system designed to detect malicious "Like" patterns that requires an additional confirmation for pages that trigger this mechanism.

<https://www.facebook.com/facebook/posts/207321425975188>

Facebook: Virus Bulletin keynote

October 2010

I delivered the keynote address at the annual Virus Bulletin anti-malware conference, VB2010 in Vancouver, Canada. In the keynote I presented a brief overview of Facebook security organization, followed by a run-down of common Internet threats and their specific effect on Facebook, with focus on Koobface and other Facebook-specific malware families.

Facebook: Malware Roadblock

May 2010

I extended and supported Facebook's remediation solution for malware infected users – the Roadblock. I worked with partners daily to ensure Roadblock was effective against all Facebook malware threats: https://www.facebook.com/note.php?note_id=10150174826745766

SonicWALL: Cloud Antivirus

January 2010

I was involved in the design and implementation of the patent-pending technology behind the "cloud antivirus" feature in SonicWALL's Email Security appliances. PostgreSQL, Linux, C++.

<http://patents.com/us-20110016527.html>

SonicWALL: Botnet Interactions Diagram

February 2009

This project aimed at presenting in a visual format the results of my research of top botnets in the world and the "bad actor" groups behind them, and charting their interactions. See the diagram at:

<http://nickolay.ca/botnets.html>

SonicWALL: SonicALERT

February 2008

I was responsible for running the public company's research blog, featuring new content about malware threats weekly. <https://www.mysonicwall.com/sonicalert/sonicalert.aspx>

SonicWALL: Antivirus Honeypot

June 2007

I set up scripts and hardware to capture malicious traffic from the Web. Traffic was gathered, viruses extracted, sorted and forwarded to the virus lab for analysis.

FortiGuardCentre research portal website**March 2005**

I was involved in concept generation, design and implementation of a major corporation's research portal. Special applications were incorporated, e.g. the online virus scanner, web addresses URL lookup, global threats statistics, and more. See the site at:

<http://www.fortiguardscenter.com>

Fortinet: Antivirus Cross-Scanner Interface**March 2004**

I installed 9 antivirus products on the server and created Perl scripts to download and install their antivirus pattern updates automatically. The users could submit a file to the server via HTTP upload, and the cross-scanner was run [the file was scanned with all available antivirus vendors products at once]. Each virus scanner ran in parallel on different client machines, then log was parsed and results were combined under one interface and stored in the database. Similar to <http://www.virustotal.com/>

Fortinet: Clean Collection & False Positive Testing**May 2004**

False positive happens when a clean file is reported incorrectly as a virus by antivirus software. The only practical way to fight false positives is to use a comprehensive clean file collection. I built the collection and the database-driven interface to allow a virus analyst to submit a test pattern and scan the whole collection. Three analyst teams from different countries (Canada, France and China) were able to test their antivirus patterns and avoid false positives. Linux shell scripts, Perl, PHP were used.

Fortinet: Virus Auto-Replication System**June 2004**

I used Perl and C++ to create a virus Auto-Replication system that is controlled remotely via the Web. First, a snapshot is taken of the computer system, and then a virus is executed. Another snapshot is taken and compared to the original. All changed and newly created files (**replicated samples**) are added to the database. The system is then rebooted, and a clean image is restored to reset the environment.

Fortinet: Performance Test Automation**October 2004**

I automated performance testing of Fortinet security appliances by creating Perl scripts that tested virus detection on all supported protocols (HTTP, FTP, IMAP, POP3, and SMTP).

SFU: Distributed Ray Tracer**November 2003**

For this school graphics project I used C++ , STL, OpenGL and VRML to implement a working ray tracer with some classic and some distributed features, e.g. reflection, transparency, anti-aliasing, textures, etc. The size of the project was over 6500 lines of C++ code.

Other School projects: <http://nickolay.ca/projects.html>

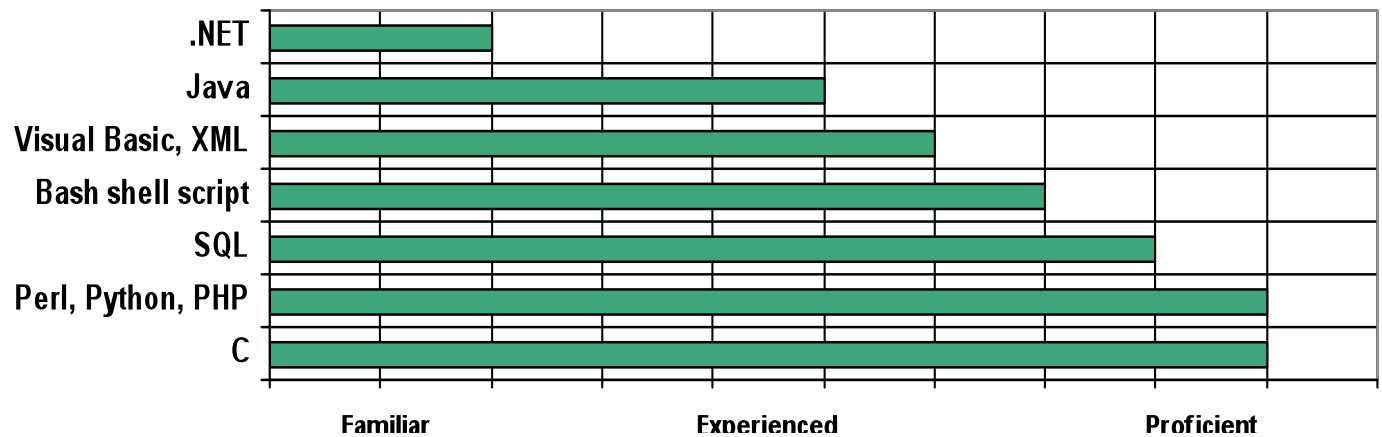
Microsoft Content Management Server Setup**July 2001**

As an intern, post acquisition, I rewrote the installation module for **NCompass Resolution** in a newer version of *InstallScript* language to be compatible with Windows Installer Technology and included the re-branding changes required by Microsoft to adopt the Content Management Server as one of MS products. http://en.wikipedia.org/wiki/Microsoft_Content_Management_Server

Skills

I am skilled at reverse-engineering, static and dynamic malware analysis, disassembly, debugging, writing patterns and tracking malware, networking, research publications and conference presentations, and representing the company at international events.

Programming



Software & Hardware

- ⇒ Security: OllyDbg, IDA Pro, Wireshark, VMWare, Snort, tcpdump, nmap, nessus
- ⇒ Web vulnerabilities: XSS, CSRF, SQL Injection, Clickjacking
- ⇒ OS: Windows, Unix, Linux
- ⇒ Web servers: IIS, Apache, Tomcat
- ⇒ MS Office (all versions), SharePoint, Exchange
- ⇒ DB: MS Access, SQL Server, MySQL, PostgreSQL, NoSQL (Hadoop, HBase)
- ⇒ Visual Studio, Borland C++, Turbo C++, gcc & makefiles
- ⇒ Adobe Flash, Photoshop, PageMaker, ImageReady, Premiere
- ⇒ HTML5, DHTML, JavaScript, Jscript, VBScript, ASP, ColdFusion, JSP, AJAX, OpenGL
- ⇒ SourceSafe, Perforce, Subversion, CVS, Git

Soft Skills

- ⇒ Excellent business and interpersonal communication skills
- ⇒ Fluent in English, Russian and Ukrainian
- ⇒ Business sense – make sound decisions for company's benefit
- ⇒ Leadership – manage people and resources efficiently to achieve deadlines
- ⇒ Certifications: GREM – (SANS GIAC Reverse Engineering), Red Cross First Aid, CPR

References

Available upon request