

Interview: Iliia Kolochenko, CEO of High-Tech Bridge

The Ethical Hacker Network is an online magazine with a focus on those in the profession. It's wonderful to have technical content, videos, book reviews and an active discussion forum, but what good does it do if we can't help our readers achieve their career goals? Being an "online" magazine also means that we have a wide audience not confined within the borders of the United States. How can we also help our international audience? One way to answer both questions is to continue our ongoing series of interviews with ethical hacking movers and shakers. So here is another conversation with someone who can provide some quality insight to the questions posed above, because he did it. He became a professional ethical hacker in Europe.

Iliia Kolochenko is the CEO of High-Tech Bridge, a security services and research outfit in Geneva, Switzerland. But clearly he wasn't born a chief executive. Just like most of us, he grew up dreaming of being a hacker, even if he had no idea it was an actual profession. This is his story, and it was quite surprising to see just how similar it sounds. But that's not a bad thing. He took his passions, combined them with his military skills, added in a little workplace frustration, and... Well you'll just have to find out for yourself.

Discuss in Forums {mos_smf_discuss:Editor-In-Chief}

Thank you so much for taking the time to share your story with the EH-Netters from around the globe. Before we get to some of the cool things your company does, we like to start things out from well… the beginning. OK, so maybe we won’t go back quite that far, but we do like to know how you got to where you are today. That being said, let’s jump right into the interview.

1. What work experience did you gain and how did that prepare you at all for starting your own company?

Since the age of 16 I was interested in computer security. Before High-Tech Bridge I was working as a penetration tester and manager for an ethical hacking company in Geneva, performing many complex projects mainly for Swiss financial institutions. I wanted to change many things in the company for the benefit of customers, company and employees. However, the management was quite unreceptive and was looking only for profit maximization. This is why after my military service I decided to start a company with a different vision, oriented for stable and organic growth, where innovation and customer satisfaction are the main priorities. Today I mainly take care of our corporate strategy and business development, participating from time to time in technical projects to personally control the quality and maintain my technical skills. My technical background is very useful, as only being a professional hacker in the past you will be able to efficiently manage hackers in the present.

2. Can you share with us how your service in the military helped in your career in information security?

It was extremely useful to develop such skills as self-organization, resistance to stress and the ability to never give up. Military service also reinforced my ability to make difficult decisions and assume the responsibility for them.

3. Who was your first client and what did you do for them?

It goes to the very beginning of 2008 when High-Tech Bridge employed 2 persons including me. It was a pharmaceutical company who had just implemented a new web application and wanted to test its security. I clearly remember how I was verifying each line of our offer again and again before sending it. Today we have complex in-house software that builds personalized offers saving a lot of sales manager’s time, but at the beginning everything was 100% manual. I remember how I was surprised when we won the tender and got the contract. We did an impeccable job spending much more human days on the project than we actually sold. However, the customer was so happy with the report quality and content that we continue working with him today.

4. How is running your own internal research team beneficial to the company as a whole?

Security research is a crucial part of our business, necessary to provide customers with high-quality service. Since the creation of High-Tech Bridge we paid a lot of attention to this department and invested a lot into it. Our researchers spend most of their time on in-house security tools development, exploit coding and searching for new attack vectors. Their efforts enable us to deliver cutting-edge penetration testing and auditing. Internal research differentiates us on our home market in Switzerland and makes us competitive on the international market as well.

5. Speaking about exploit coding, does that also include exploits for 0day vulnerabilities?

We intentionally don't spend much time searching for 0day vulnerabilities. High-Tech Bridge's business model and clientele needs are different from business the model and clientele needs of such companies as Vupen, a leading company in the domain of vulnerability research and 0day exploit creation. We deliver independent and high-quality security testing based on risk classification and prioritization. Risk of 0day vulnerability exploitation in a well-known product is very low in comparison to other risks, such as unpatched vulnerabilities, insecure system configuration or weak links in the corporate security that were not taken into consideration while building security perimeter. Of course, if we find a 0day vulnerability during a penetration test, we inform the customer about it and recommend an intermediate solution to prevent exploitation. But 0day vulnerabilities are not what our customers are mainly looking for, this is why we give preference to development of universal exploits for public vulnerabilities for which exploits are unavailable.

6. How does High-Tech Bridge protect its clients against 0day vulnerabilities?

You can be reliably protected against a 0day vulnerability only if you possess it. However, professional system hardening can prevent many exploitation vectors of 0day vulnerabilities making them almost unusable. Nevertheless, it is always a question of money and time. If your rival is ready to spend millions on compromising your system, one day or another he will succeed. The problem is that the cost of protection is much higher than the investment necessary to compromise your system. Professional black hats will rarely start the attack from your frontal systems. They would rather find a weak point in your information system perimeter that may consist of employees working from home, your partners, suppliers, lawyers and other trusted parties who have access to the confidential information the black hats need. Usually security of such third parties is much weaker than your frontal systems security and can be bypassed quite quickly even without a 0day. This is why we always advise our customers to have a global vision on their information security taking into consideration all possible attack vectors and entry points.

7. Your Security Research Lab released hundreds of security advisories that cover many well-known software products. Can you tell us a little bit about it?

High-Tech Bridge Security Research Lab, a unit of our R&D department, was created at the beginning of 2010 to help software vendors improve the security of their products on a non-profit basis. We consider it as our social responsibility. One of the first advisories was XSS vulnerability in Microsoft SharePoint 2007 that made a lot of noise after public disclosure, as an official patch from Microsoft was not available yet. Disclosure without patch was our fault as we just started this type of activity and our experience in the vulnerability disclosure domain was very modest. Since then our advisories were continuously improving, ameliorating communications with vendors and many other important aspects. 2012 was a crucial year during which High-Tech Bridge Security Research Lab obtained CVE and CWE Compatible status. Many improvements were made thanks to the help of Brian Martin, COO and President of Open Security Foundation (OSF). His unique experience in vulnerability management was very helpful for us. Today Brian is a High-Tech Bridge Advisory Board member who still contributes a lot to permanent perfection of our advisories.

8. Do you think it is important for an ethical hacking company to perform internal security research?

It is not just important, it is crucial. Without it you would simply not be able to deliver high-quality service to your customers, be it penetration testing or forensics. Today the demand for ethical hacking is growing and supply follows. As a result we have many self-proclaimed experts and ethical hacking companies without any experience on the market, selling poor Vulnerability Scanning under the guise of manual Penetration Testing, spoiling the image of the ethical hacking industry. Newcomers usually try to focus on profit maximization and not on their customer's needs. This is the worst.

9. So, what advice can you give a customer who is trying to identify a competent or 'ethical' ethical hacking company?

Each case is pretty unique and depends on many factors, but I can highlight some important points one should carefully verify before hiring an ethical hacking company. First point is to have total vendor and product independence - ethical hacking companies who resell and/or integrate third-party security products cannot guarantee the main values of security testing: neutrality, objectivity and independence. Second important point is experience in the ethical hacking domain of at least several years. Today some large IT companies try to follow the fashion and start offering ethical hacking in their portfolio of services without really understanding which market they enter. The third point is the number of security certifications that a company and its employees have. However, one should not rely only on certifications, as some of them are quite easy to obtain and cannot assure anything. The last point, which I have already mentioned in our discussion, is solid security research. I highlight the word solid, as some security companies tend to create a poor XSS scanner that misses 90% of XSSs and then proudly claim to have proprietary cutting-edge security software. I would recommend reading the Frost & Sullivan analysis of the ethical hacking industry that provides clear and simple guidelines on how to select an ethical hacking company.

10. Sounds like there are similar issues in Europe as there are here in the States. Can you shed some light on other areas where the European market may pose challenges or may be different from the US market?

I will not speak for the entire European market, as each country is quite different. However, talking about the Swiss market I'd say that the main difference with other markets is market stability. It is extremely difficult to enter the market if you are a newcomer, as you may visit a customer year after year before he will finally sign. However, once you sign a contract and manage to deliver professional service and follow-up after - you have very good chances to become a long-term security partner of the customer. Even for High-Tech Bridge, a company consisting from experienced Swiss security experts, it was a big challenge to gain customer's trust that took us several years.

11. High-Tech Bridge offers a wide range of highly technical services. But with the growth of not only threats but the regulations requiring all organizations (including some small ones with even smaller budgets) be compliant, what can be done to service SMBs that may not be able to afford the type of hands-on, personal attention that pen testing or red teaming can provide?

Fortunately SMBs usually don't fall into the category of companies that must perform complex and frequent security assessments. However, it's not a question of legal compliance but of business continuity and safety of corporate intangible assets and intellectual property that may cost a fortune. Today, one of the weakest links in corporate security is a corporate website that serves as an open door to the internal network. Frost & Sullivan, in collaboration with MITRE, OTA and High-Tech Bridge, released a White Paper about web application security that clearly explains all of the dangers of vulnerable web applications. SMBs often fail to secure their websites properly due to complexity and the high price of the process. To change the current state of affairs and resolve this problem, at High-Tech Bridge we have developed ImmuniWeb® - an innovative web application security assessment product with a SaaS delivery model.

ImmuniWeb® enables one to assess his website security and reliability in a simple and highly-efficient manner. ImmuniWeb® will be publicly available very soon.

12. Does it mean that SMBs are the main audience for ImmuniWeb? Can penetration testers also use it?

No, I cannot highlight SMBs as main customers for ImmuniWeb®. Multinational corporations and governmental structures will also be able to leverage its unique concept to assess security of their web applications in a highly efficient manner. Talking about its usage by penetration testers, I can only say that ImmuniWeb® is a self-assessment tool that is not designed to perform security assessment by third-parties.

13. The Ethical Hacker Network not only produces technical content, but we also pride ourselves in providing career guidance and inspiration. For our final question, if you could give our readers one piece of inspirational advice, what would it be?

My main advice is to do what you really know how to do and what you really like to do. And never give up even in hopeless situations. Simply because hopeless situations do not exist, there is always a solution - you just have to find it.

Excellent advice and very appropriate not only to our industry but also when making the transition from taking orders to giving them. I've often said that in life and in work, one must be able to lead and be lead.

Thank you very much for your time. Please keep us informed when ImmuniWeb® is ready. We'd definitely be interested in taking an early look and sharing an insightful review with our readers.

Donald C. Donzal

Editor-In-Chief

The Ethical Hacker Network

www.ethicalhacker.net