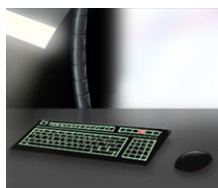


23 February 2009

By: Lucian Constantin, Web News Editor



HackersBlog
interviewed by
Softpedia
HackersBlog

[Hackers of Kaspersky, Bitdefender, F-Secure and Symantec Speak Up](#)

Softpedia exclusive interview with the HackersBlog crew

During the past few weeks, a Romanian self-proclaimed ethical hacking group has kept the leading antivirus vendors on their toes after disclosing SQL injection vulnerabilities on several of their websites.

The security companies that have been affected include [Kaspersky](#), [Bitdefender](#), [F-Secure](#) and [Symantec](#). Even though some vulnerabilities have been less serious than others, these documented attacks have strengthened the idea that security is a cat-and-mouse game and that, indeed, no one is invulnerable on the Internet today.

The acts of these Romanian hackers have attracted a lot of media attention and have raised enough controversy. Who are they? What do they want? Why do they do this? Why are they after AV vendors? - these are all questions that many users might have contemplated while reading the news stories.

Therefore, driven by curiosity and armed with lots of questions, Softpedia has gone hunting for some answers and contacted the HackersBlog crew. Much to our surprise, at the other end of our "weapons" we have found people who are open to dialog and do not hesitate to speak their minds. If you're as curious as we have been, please read on to find out what we have dug up.

Softpedia: By now, everyone has become curious as to who you are. Obviously, we're not going to ask for your real identities, but more like what you do for a living. Is any of you working in IT security as a penetration testing professional or similar, or are you just hacking enthusiasts?

HackersBlog: We are just passionate about IT security. Some of us work in IT but not particularly in security. We are mostly into web and software programming.

Softpedia: How did your group come to be? Did you know each other since before HackersBlog was set up? And while we're at it, can anyone join your group? Please elaborate.

HackersBlog: The name of the blog (United) speaks for itself. We come from different hacking groups and we have decided to put aside personal misunderstandings and unite for a greater cause. Luckily for the rest of the people, this union has not been based on an idea of destruction and mayhem oriented towards companies and websites, but on cautioning users about the dangers out there on the Web, as well as putting programmers on guard regarding the security flaws we find in their pages. This group is not limited in number, and we are open to anyone who will show that they can bring value to the group. The most important thing, though, is for them to share our principles and report the problems they find to webmasters, without misusing any unauthorized permission gained or resource accessed.

Softpedia: So far, most if not all vulnerabilities disclosed on HackersBlog have been Web-related. Do you tend to focus on Web application security? If yes, are you considering expanding your range in the future?

HackersBlog: Lack of time is our main obstacle and this forces us to focus mainly on Web applications for now. It is possible that we will expand our views into other areas, in the future.

Softpedia: The published proof of concept attacks that attracted the most media attention were based on SQL injection or cross-site scripting (XSS). Do you also document other types of Web attacks such as cross-site request forgery (CSRF) or UI redressing (Clickjacking)?

HackersBlog: CSRF and clickjacking are somewhat inter-related with XSS attacks. While CSRF attacks are already widely known by the public and are heavily used in browser exploitation, we cannot say the same about clickjacking attacks, where things are still in their incipient phase. We will wait out to see how things develop with this kind of attacks before publishing anything about them. It would be a waste of valuable time to post explanations and tutorials that can already be easily found on the Web. Jeremiah Grossman and his team do an amazing job, and we take great pleasure in reviewing their work as often as we can.

Softpedia: Kaspersky has challenged your code of ethics, claiming that you have only given it one hour on a Saturday to address the problem on its US support site before going public with it. How do you respond to that? What does "timely manner" mean according to your own standards?

HackersBlog: First of all, let's set the record straight from the start! That problem should have not been there in the first place! Their complains about our "timely manner" are pitiful and shameful. They had about a day to take action. From our standpoint, one hour should be more than enough for a site of the caliber of Kaspersky, let aside the fact that it was bad that it was there, as we previously mentioned. Therefore, when it comes to such companies, a "timely manner" gives them more than just that.

Softpedia: You published a disclaimer on your website in which you advised that you would not disclose any sensitive information obtained as a result of successful exploitations. The guys at Kaspersky said that you were more interested in fame than in causing damage. Are you doing this for publicity?

HackersBlog: We just want to shed light on security problems on the web and make people understand that the Internet is not just some playground, but can be a major eagle eye into our private lives. Remember that our actions are non-profit and any publicity will not bring us any money, rather the opposite.

Softpedia: In less than two weeks, four antivirus vendors sustained attacks from your group - Kaspersky, Bitdefender, F-Secure and Symantec. Should av vendors and security companies in particular be on their toes for similar attacks from your group? Are you trying to make a point by targeting them?

HackersBlog: We didn't make a habit out of testing AV websites. We thought it would only be fair to show people that other companies have similar issues. We wanted to make it clear that Kaspersky was not the only one out there facing this kind of problems, and we didn't want to single them out.

Softpedia: Security vendors strongly recommend that companies and webmasters implement strict code review practices in order to prevent such data leaks. Does this sound hypocritical to you now, given that your actions prove they are just as vulnerable as anyone else?

HackersBlog: We are sure that those recommendations are made with the best of intentions in mind, both for protecting the privacy of their users, as well as for preventing undesirable situations for webmasters and companies from happening.

Softpedia: In addition, security vendors claim that when data breaches do happen, affected parties should be as transparent as possible and assume responsibility. How do you think the four affected antivirus developers have handled themselves in this respect? On the same note, what do you think of Bitdefender's reaction, which has downplayed the attack on its partner's website, even though it sells its products and uses its branding elements?

HackersBlog: It seems that Kaspersky's image was, by far, the most affected. We didn't expect that our disclosure would have such a devastating impact on them. We had no intention of undermining or affecting their public image in any way. Their AV products are very efficient and it would have been wonderful if their web interface had gotten the same attention as their security products. We think that F-secure and Bitdefender had it easier simply because all eyes were on Kaspersky at the time.

[Bitdefender.pt](#) was, indeed, a partner site. Still, nobody cares about this detail, which becomes minute the more you dig into it. As long as they had the Bitdefender logo all over the place, as long as they were selling ONLY Bitdefender products, and as long as the name of the website was Bitdefender, who would consider such an insignificant detail as the fact that it was a partner site? Needless to add, the website contained client data and the vulnerability would have made that available to anyone.

The guys at F-Secure.com seem to have had the best approach to the issue. They admitted they had a problem, they disclosed exactly what happened and that they looked at it as a lesson they learned from how to protect their website.

Symantec [said](#) that its vulnerability was not effective at all. Whether or not the problem came from its error-handling routines, Blind SQL techniques could have been used to extract pieces of information from the database, by interpreting the different responses received from the server in case of an error / no error. It would have been pure insanity for an attacker to extract items of information with this technique, but still, the vulnerability was real.

Softpedia: Finally, tell us a few words about what drives you to do what you do. Give us some insight into your future plans. What should we expect from HackersBlog next?

HackersBlog: We will do what we know best. We will publish more articles that will disclose vulnerabilities on (some major) websites. We hope that people will soon realize the fact that

this kind of actions are beneficial and we also hope they are able to make a distinction between our research and black hat attacks, which are increasing web-wide. Right now, the general public is not yet aware of the destructive power that the Internet facilitates for anyone with just a little knowledge but the drive to do harm. We are aiming at opening their eyes and calling their attention to taking steps towards protecting themselves.

Softpedia: Thank you for taking the time to answer our questions, and we hope to write more interesting news about your achievements in the future.

HackersBlog: Thank you for your interest in our activity and also for giving us the opportunity to share some of our thoughts with your readers. Knowledge is power only when applied. We hope to have an open dialog with anyone who wants to know more about our mission.