

# Lost Interview with the Deceptive Duo

© 2002-2004 Cyrus Peikari

Feb. 1, 2004

Published at <http://www.airscanner.com>

Please do not redistribute without permission.

In 2002, a pair of hackers who called themselves the "Deceptive Duo" went on a website defacement spree of high-profile government computers. In this case, however, there was a twist: the Duo stated that they were hacking as "patriots" in order help their country after 9/11. According to the Duo, their purpose was to raise public awareness in order to help mitigate future terrorist attacks from abroad. In this endeavor they were successful. After carefully redacting any sensitive information, the Duo prominently displayed examples of critical databases that they had penetrated. This included personal information of airline employees such as names and addresses.

Was this the work of domestic terrorists, or should the Duo be celebrated as patriotic heroes? The truth probably lies somewhere between these two dramatic extremes. Whether you consider them as minor vandals, or as patriotic activists, one thing is for sure – don't try this yourself.

To the best of our knowledge, there has been no public statement by the Duo since their capture. In some cases like this, after being captured the defendants agree hack for the government (and the government is glad to have them) in exchange for leniency. Judging by the "patriotic" statements before their arrest, nothing would make the Duo happier.

This seems to follow a recent trend that we have seen among young hackers. Some of them have told us they would like to become "notorious", even arrested, in order to help their future careers. They have cited examples to us of former hackers who know are well known in infosec because of their past crimes. Specifically, they have referred to Kevin Mitnick (founder of Defensive Thinking) and Kevin Poulsen (editorial director at Security Focus), both of whom achieved notoriety after serving jail time for hacking.

While it is true that Kevin Mitnick and Kevin Poulsen are both successful and talented, we do not recommend that young people follow in their footsteps when it comes to their earlier crimes. There are better ways to establish yourself in the infosec field.

A few days before their arrest and capture by the FBI, we approached the Deceptive Duo through their defacement email and they were kind enough to grant an interview. The following is one of the last public interviews given by the Deceptive Duo shortly before the FBI raided them. The date of this interview is May 2002. It is published for the first time here, almost two years later.

[Interview with the Deceptive Duo:](#)

**Q: How did you get started in Internet security?**

A: We learned how to program, which allowed us to understand how many things operated. From there, Internet security was a must. It was forced on to us in a non-intrusive way. You can never really explain these types of things, it just happens. The Internet was at the forefront of computing, and it still is. Security in this area was surely to be focused on.

**Q: What websites have you penetrated?**

A: Some of the high profile computers that we penetrated included: Midwest Express Airlines, the Space and Naval Warfare Systems Command, the Office of Secretary Defense, the Defense Logistics Agency, NASA Jet Propulsion Laboratories, Sandia National Laboratories, and more.

**Q: Why do you feel defacements are necessary?**

A: Defacements are necessary because of the non-chalant response we receive when notifying a system administrator of the breach. It takes action to get reaction. It also shows others who witness this, the situation we are facing. We remain vulnerable, and the public needs to know this.

**Q: Which do you feel is the least secure operating system: Linux or Windows**

A: It highly depends on the competence of the system administrator. You cannot judge a book by its cover, just as you cannot judge a network by its product. Windows can be just as secure as Linux, and Linux can be just as weak as Windows.

**Q: How old were you when you first got started in Internet security? How old are you now?**

A: At this time we cannot divulge any information pertaining to our personal lives.

**Q: Do you feel that your methods are illegal?**

A: We believe it is illegal, to an extent. But we must sacrifice to gain. We are putting our futures on the risk in the name of US National Security, the public's safety.

**Q: Who are some of the individuals or groups you look up to?**

A: We look up to anyone who stands up for something.

**Q: What are your favorite software tools?**

A: Our favorite tools are Notepad, vi and NMAP.

**Q: What are some resources that you recommend for readers to learn more about Internet security?**

A: The greatest resource lies within you. Trial and error works the best. Just continue reading, keeping yourself up to date. We highly recommend [www.securityfocus.com](http://www.securityfocus.com) and [www.securiteam.com](http://www.securiteam.com) as a place to read.

**Q: How would you describe the current state of Internet security?**

A: We'd rather act on it and do something about it, than speak about something that we all know is truly insecure. The Internet is a vast region, a place that will always be insecure. For that reason, we can only shape it into a better place. As secure as POSSIBLE.

**Q: What solutions do you foresee for the current problems in Internet security?**

A: Determining the end of something would be utilizing psychic powers, which we do not have. It's something that can't be accurately predicted.

**Q: Where do you see yourself in the future?**

A: Hopefully, in a more secure environment.