



THE MALWARE REPORT

New Delphi Virus Uses Old School Methods

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: New Delphi Virus Uses Old School Methods

Episode: 136

Location: http://www.eset.com/podcasts/082009_ESET_Delphi.mp3

August 27, 2009

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant, and you're listening to The Malware Report with Randy Abrams. Hi, Randy, how are you today?

Randy Abrams: Excellent, thanks. How are you?

Matt Grant: Good, thank you and thanks for joining us. You know, recently I know the security research community has been seeing something unusual in the malware world and that's a virus that's targeting a development environment. I guess this virus that's been dubbed the Win32.Induc was written to infect applications built with Delphi. Can you tell us a little bit more about this particular virus and what Delphi is?

Randy Abrams: Sure and actually I'm not positive that's pronounced Delphi or Delphee, but we can go with Delphi for this conversation.

Matt Grant: Sounds good.

Randy Abrams: Delphi is a programming language. So, people write applications like word processors, chat clients, spreadsheets, any kind of program that you want can be written in this programming language. So, that's what it's used for. It's kind of like C or visual basics or any other programming language. But one of the interesting things about this is, when the file is infected, it doesn't infect other executable files. Your standard, old school virus would go from executable to executable and this one instead is what it does is it looks to see if the Delphi programming environment is installed on the computer and if it is, then it makes a modification so that every program the developer writes, is infected with the virus. So now, when customers get files that are compiled with Delphi, that means they take the code the programmer typed in and make it into a program, when they get these programs that are infected, if they don't have the Delphi, what they call IDE (Integrated Development Environment) installed on their computer—which most average users don't—the virus doesn't do anything. That's a real interesting kick back to very old school virus writing where a lot of the virus writers in the old days weren't interested in stealing money or causing damage, they just wanted to prove a concept or something. So, for the average user, essentially it's not a problem other than virus writers that aren't in it for money don't often quality control their work so there could be compatibility issues. But for a software development house, this could be a big problem because it damages your reputation to have a virus in your code, even if the virus doesn't do anything harmful. Believe me, I speak from experience because I worked at Microsoft and I was responsible for making sure that Microsoft didn't release infected software. The one that got past me was a virus that was not going to infect anyone because it was so deeply nested in an area that nobody could get to without trying really hard that it never infected anyone, but the code

itself was infected. It was a bad PR hit for Microsoft and, as a result of that, I got antivirus companies to detect some new file types that they never decompressed before. The other really interesting thing about this is a lot of the bad guys that are riding banking Trojans, which are really prevalent in Brazil and Russia, got infected. And that means that if they don't check, we don't have to detect their new creation based on it being a banking Trojan, we can detect it because we know the Induc virus and detect that; so that gives us two vectors to detect the program. It gives the whole antivirus industry two sectors to detect these malicious programs.

Matt Grant: Interesting. So, I guess, what do you think the overall goal was then with developing this virus?

Randy Abrams: I'm pretty sure the overall goes was somebody having fun wanting to prove a concept.

Matt Grant: Interesting. And I guess, can you explain a little further then how it would get from machine to machine?

Randy Abrams: Well, one of the ways we've seen it spread actually is through peer-to-peer networking. Things like Kazaa or Juarez where people are downloading illegal software, that's one of the ways. Another way is like the banking Trojan like I said. People go to a website; it could be a drive by, it could be a phishing email, it could be a trojanized program that someone downloaded, there's a variety of ways that that could happen. It potentially could infect a file that uses Windows AutoRun and spread via USB because it doesn't care what program it infects as long as it was written in Delphi, then it infects it. So, it doesn't spread from executable to executable though. So, its kind of interesting the number of infected files we've seen considering that the program only infects really the development environment and then it's the programs that compiled that are written by people that come out infected.

Matt Grant: It doesn't seem to be doing anything malicious, so what is it doing and is there a concern I guess for the general public to be worried about this virus?

Randy Abrams: There's a concern if you're developing in Delphi. There's concern because of reputation. In terms of losing personally identifiable information, bank account information, stuff like that; there's not really a concern for this virus, but you can bet the copycats are going to grab this and especially the bad guys are going to grab this and build in the ability to steal information. So, while this one is relatively harmless to the average user, the next one can have all kinds of different capabilities.

Matt Grant: Absolutely and that's a good point. Thanks, Randy for taking the time to explain this particular virus to us in further detail. If you're interested asking Randy any questions about this particular virus or anything else, feel free to e-mail him at askeset@eset.com. You can also follow Randy on Twitter @esetresearch. This has been Matt Grant and you're listening to the Malware Report with Randy Abrams.

[End of recorded material]