



## **THE MALWARE REPORT**

### *Waledec Worm the New Storm?*

#### **Participants:**

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

#### **The Malware Report Transcript**

Title: Waledec Worm the New Storm?

Episode: 115

Location: [http://www.eset.com/podcasts/031709\\_ESET\\_Reuters.mp3](http://www.eset.com/podcasts/031709_ESET_Reuters.mp3)

April 2, 2009

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant, and you're listening to The Malware Report with Randy Abrams. Hi, Randy. Thanks for being here.

Randy Abrams: Hi Matt. It's great to be back.

Matt Grant: I wanted to spend a few moments today talking about the latest attack by the Waledec Worm. It seems like this latest wave is personalized virus attacks sent through email that blasts out fake news alerts about shocking events that supposedly happen in or around a particular recipient's hometown. Can you tell us a little bit more about this attack?

Randy Abrams: Sure. What this is doing is advancing social engineering. The whole object of social engineering is getting people to do something they normally don't want to do, but think they want to do. In this case, it's

so that they'll install the virus, click on links and things like that. So, one of the best ways to trick people into doing things is make the message seem relevant to them. I know that you live, or my program knows that you live in San Diego; if I send you a news story about San Diego, it's more contextual, it makes more sense to get something from San Diego than you would get something out of the blue from a tiny town in Norway.

Matt Grant: Absolutely. How are they doing this type of geo-location?

Randy Abrams: I haven't actually spoken with our research team about the technique used, but I can take a pretty good educated guess. Your IP address gives a lot of information about where you're at. Now it's not foolproof because there are proxy servers and things like that that will use a different IP address. In San Diego, Comcast will have a range of IP addresses; here in Seattle where I live, Comcast has a range of IP addresses. All the ISPs use IP addresses and they're tied to the location. It's fairly easy to know the IP addresses of a computer, a program can figure that out automatically. Once they have that information, they know what area you live in and what the close metropolitan areas are. By having that information they can target the email so it says, "Jet crashes in San Diego airport," or something like that. The sensationalistic headlines blow up, people have to see it - "I gotta see it." The more they see it, the more they want to read it. My educated guess is that's how Conficker is using GeoIP which is an interesting thought because if you look forward as mobile devices become more ubiquitous and have actual GEO built into them, you're not spoofing it, you know exactly where they are at. There are some interesting implications going on.

Matt Grant: Interesting. The threat I have seen is appearing as a Reuters breaking news alert. Is it just Reuters they're using as the news alert or are they

using other news organizations as well? How can you tell the real alert from the attack?

Randy Abrams: One of the first signs is that you got the alert. If you didn't sign up for a news alert from Reuters or other news organization it claims to be from, it's fake. They're not going to send you these news alerts you never signed up for; how foolish could you be to fall for that? You never signed up for that alert, "Oh yeah, I didn't." Another thing to look at is what the link really is; where does the URL take you to? If it isn't going to the news organization itself, then there's a very strong probability this is fake. The probability approaches 100 percent. Look at what you're clicking on and where it's taking you to, those are some of the top ways. Another great thing to do is keep your antivirus software updated so that it gets detected coming in using anti-spam; anti-spam will filter out a lot of them as well

Matt Grant: Some are saying the Waledec Worm is the successor to the Storm Worm, do you agree with that?

Randy Abrams: I think that's kind of abusing the term successor. I kind of think of it as a monarchy or dictatorship where something is passed down. I don't think Waledec was passed down from the Storm. It could have been created from the same author; I haven't looked at the indications for that. The Storm Worm hasn't gone away, it's not stepping down. Waledec is the big one that's getting a lot of attention and there will be others after Waledec as well. It makes interesting commentary, but it's irrelevant on discussing which is the "Big One," people just need to take the proper steps to stop letting these things spread.

Matt Grant: Well Randy, I appreciate you taking the time to speak with us today about this latest attack. If you have any questions for Randy please feel free to e-mail him at [askeset@eset.com](mailto:askeset@eset.com). This has been Matt Grant and you've been listening to the Malware report.

[End of recorded material]