



THE MALWARE REPORT

April Fool's New Conficker Variant Arrives April 1st

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

The Malware Report Transcript

Title: April Fool's New Conficker Variant Arrives April 1st

Episode: 114

Location: http://www.eset.com/podcasts/031709_ESET_Conficker.mp3

March 26, 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 talk today about the Conficker Worm. I know that we had this discussion a month or so ago, but it does seem there have been some reports that the Conficker Worm is set to explode on April Fool's Day. A variant of the worm, which kills protective security processes, is going to activate on April 1st. Have you heard anything about this?

Randy Abrams: I've heard about this. There's a new variant - Conficker.C or some companies call it Downadup.C. This version is supposed to activate on April Fool's Day. It's going to do some things like disable security software so it goes undetected. It's not just antivirus software, this

thing is going after programs like Wireshark; Proxmar, a process monitoring tool; TCPView, people use it to view what's happening on their TCP/IP connection; and Redgemont, which monitors registry stuff like that. The biggest change in it is its domain registration algorithm.

Matt Grant: Before we get into some of the specifics regarding this variant, can you just give us a quick overview of Conficker?

Randy Abrams: Sure. Conficker was launched to exploit a vulnerability that Microsoft has since patched and a lot of the problem is people aren't patching like they should be, especially in some corporations it seems because at the beginning at least we saw Conficker mostly hitting the corporate arena. It also does things like use autorun to install itself - there's a danger there. It spreads to network resources as well - it's got multiple attack vectors. Once it's on there, it checks with various Web sites that it automatically has registered to see what it's supposed to do next. So it's susceptiblely a bot.

Matt Grant: Interesting. So going back then about this particular variant using domain registry. Can you give us a little more details about Conficker.C?

Randy Abrams: Sure. With the prior versions of Conficker, what it did was it had a domain generation algorithm and what that does is that it knows that it's going to need to get instructions. To get the instructions, it's going to need to go to a Web site for them. If they hardcoded the Web site, then the security researchers would know what the Web site is and be able to shut it down and that's not in the author's best interest. So it has an algorithm that will automatically generate domain names and the author knows what those will be in advance, so the author can register the domain names and get the instructions all set up and the infected computers will update themselves. The original versions generated 250 domain names a day - these are Web sites. With

Conficker.C, instead of 250 a day, it's 50,000 domain names a day.

The idea is to make it really hard for the researchers to pre-register the domain so they can't be used because we can figure out what the domains are and get them pre-registered so they can't be used by the worm to update itself. The task is possible with 50 names a day, but when you get to 50,000 domain names a day it's not manageable. It really points to some work that Internet Corporation for Assigned Names and Numbers (ICANN), the body that provides domain names, needs to do to make it take a little bit longer to register a domain name.

Matt Grant: Yes, absolutely - especially with the increase in domain names with this particular variant. What can be done to stop this attack?

Randy Abrams: The best thing to do is not get infected.

Matt Grant: Any particular ways to best protect yourself from it?

Randy Abrams: Keep your security software up-to-date, use legitimate security software. There are a lot of pirated versions of antivirus products out there that aren't actually antivirus products or, if they are, they've been cracked so you actually infect your computer with them. Use a quality antivirus product, keep it up-to-date; use some safe web browsing habits. Don't open up email attachments unless you know they're good. That means if you get an email from someone that has an attachment in it; make sure the person actually meant to send the attachment, what it is and where it's from before you open it - just the security basics. On another podcast I mentioned www.staysafeonline.info and that's a great resource for all around techniques used to stay safer online; those are the basics. I recommend turning off autorun on Windows PC. Don't use weak passwords - Conficker will guess weak passwords and infect the computer if it has a weak password. You have to have a good password. All these steps need to be taken to protect yourself. It's not just Conficker; it's just how you protect yourself from them all.

Matt Grant: Absolutely. Really good advice, Randy. We certainly appreciate you taking the time to give us these tips and to speak on these further. If you have any questions for Randy that pertain to any of these threats that we discussed or anything security related, please feel free to e-mail Randy at askeset@eset.com. This has been Matt Grant and you've been listening to the Malware report.

[End of recorded material]