CONFICKER

How the Conficker Problem Just Got *Much* Worse

By John Mahoney, 1:00 PM on Fri Apr 3 2009, 78,979 views

On the surface, April 1 came and went without a peep from the dreaded Conficker megaworm. But security experts see a frightening reality, one where Conficker is now more powerful and more dangerous than ever.

In the first minute of April 1, Conficker did exactly what everyone knew it was going to do: It successfully phoned home for an update. And while it was fun to imagine what nasty payload that update may have included (it was fun, wasn't it?), the result was not outwardly catastrophic; rather than a blueprint for world domination, the update contained instructions on how to dig in even deeper.

"The worm did exactly what everyone thought it was going to do, which is update itself," security expert Dan Kaminsky, who helped develop a widely-used Conficker scanner in the days leading up to April 1, told us. "The world wants there to be fireworks, or some Ebola-class, computers-exploding-all-over-the-world event or God knows what, but the reality is...the Conficker developers have cemented their ability to push updates through any fences the good guys have managed to build in February and March."

And here's why that is deeply, deeply scary. As we explained, Conficker has built a zombie botnet infrastructure by registering hundreds of spam DNS names (askcw.com.ru, and the like), which it then links up and uses as nodes for infected machines to contact for instructions. In its earlier forms, Conficker attempted to register 250 such DNS names per day. But with the third version of the software, the Conficker.c variant which has been floating around for the last month or so, the number of spam DNS takeovers was boosted to 50,000 *per day*—a number security pros can no longer keep up with.

What the April 1 update did was simple: It provided instructions for linking up with the thousands, perhaps tens of thousands of new nodes registered by Conficker.c over the last few weeks, effectively growing the size of the p2p botnet to a point where it can not be stopped.

"It's not about ownage, it's about continued ownage," says Kaminsky, citing a favorite quotation of one of his hacker buddies. "It's not about how you get into the network, it's about, 'How do you be [there] a year from now?'" And the answer is: "You do a lot of the things the Conficker developers are doing."

"This is not something where the guys wrote it, it's out, then they're going to go out and play Nintendo. They're frankly trying to build something that is a sustainable network for months or years to come," Kaminsky says.

Kevin Haley, director of Symantec Security Response, raises another good point: "The first [of April] would have been a pretty bad day to choose [to do something with Conficker], because everyone was watching to see what was going to happen. Whoever's behind this is as lot more patient than we are."

As far as what comes next? More waiting. Good methods now exist for detecting and cleansing Conficker from infected machines on a network (and, let's not forget, a months-old security patch from Microsoft is all you need to protect yourself), but by now the size of Conficker's infected army of nodes spread around the world is big enough to function with devastating consequences even if most PCs are secure.

So we'll just have to keep waiting to see what this thing does.