Why Visibility And Control Are Essential When Advanced Malware Flares

Rather than focusing on the hype surrounding the latest network malware, focus on how to attain the visibility and control you need to protect your customers' assets.

By Alfred Huger, VP of development, Cloud Technology Group, Sourcefire

It seems virtually every news source is covering the new Flame worm — a recent Google search on "Flame worm" yielded over 7 billion results. As with most press-worthy malware, much noise is being made about the complexity of this threat. It takes screen shots, logs keystrokes, monitors voice communications, and compresses and transfers that data over encrypted channels to command and control (C&C) servers. While it was clearly developed by sophisticated attackers, if you take into account that it appears to be highly targeted at computers in the Middle East and seems to be driven by information stealing as opposed to a monetary incentive, it is reasonable to conclude that the author is probably a nation-state.

The good news is that from the perspective of widespread malicious intent, it is unlikely a typical user will ever be infected by Flame. In some ways, however, Flame is similar to Duqu and Stuxnet, and we'll likely see other threats that will build upon or be variants of Flame. In addition, if you look at Flame's base attributes, you can describe dozens of pieces of malware or malware frameworks infecting millions of PCs in the wild today.

Rather than focusing on the intent behind the latest advanced, highly targeted attack, we need to broaden the discussion to what to do after a malware infection happens. Most technologies today focus on detection. And although many organizations deploy multiple layers of security to catch malware, they still experience malware infections. Why? Because they lack the visibility and control to determine the 'what if?' and 'what now?'

Having visibility means addressing questions about threats or files in your environment that help you understand your exposure. You need to be able to answer questions like:

1. How long has the threat been here? This is important so you can understand the length of your potential exposure.

2. Who else has been infected? If you discover the threat from a network product (outbound communications for example), a call to your help desk, or from some source other than through your antivirus tool, how do you find where else it is on your network?

3. How did it get in? This is critical to understand. To avoid re-infection you need to address the threat at its source — how it entered your environment. If you can't do this, you'll find yourself in a never-ending game of malware 'whack-a-mole' — you know you have an infection, you have taken steps to remove it, but it keeps popping up again.

4. What did the threat do? Not all threats are equal, and it's important to understand how serious your exposure was. Did your worst nightmares get realized with sensitive data being stolen or was the threat innocuous?

If you can answers these questions, you have the necessary visibility to understand the outbreak. Now you need control to stop the outbreak. This means being able to remove the file from every instance of infection without having to wait for vendor updates. You also need to be empowered to stop the threat and its variants from getting access to your corporate assets in the future, even if your protection technologies cannot yet detect the threat.

The Flame worm is the latest in a series of what we can expect to be relentless and increasingly sophisticated attacks, some more targeted than others. Rather than being distracted by the intent — it's unlikely that Flame is easier or harder to defend against than other advanced malware — we should focus on how to attain the visibility and control we need to protect our assets in a post-infected world. ●

Alfred Huger

SOURCEfire®

Alfred Huger is the VP of development at Sourcefire in charge of product delivery for their Cloud Technology Group. He has held technical executive roles in the computer and network security industry for over 16 years and is a three-time veteran of launching successful start-up companies.

Web Exclusive