What Are Internet Worms, and Why Are They So Dangerous?

howtogeek.com/415873/what-are-internet-worms-and-why-are-they-so-dangerous

Andrew Heinzman

David Orcea/Shutterstock

We don't hear much about internet worms anymore, but they're still an important part of the malware ecosystem. But what are worms, how do they spread, and how are they used by hackers?

Internet Worms Spread like Real-World Parasites

Most malware has to brute-force its way onto your computer, either by tricking you into downloading dubious software or by piggy-backing on benign email attachments. But worms are different.

Worms, unlike viruses or trojans, take advantage of a computer's pre-existing security vulnerabilities at an operating-system level. Worms are also standalone software or files, and they typically travel across a computer network (your home or work network, for example), rather than through software downloads.

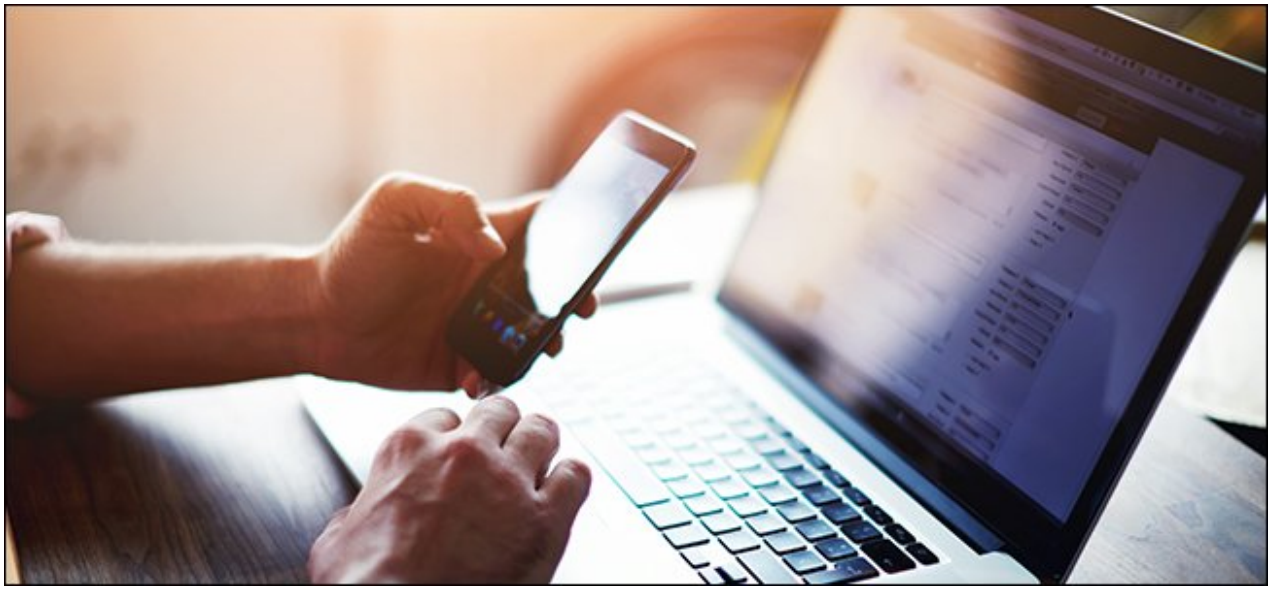
The function of an internet worm is similar to that of a real-life parasite. Like a tapeworm, an internet worm duplicates itself across as many hosts (computers) as possible, without trying to create any severe damage.

That's right; a worm won't corrupt your files or break your computer. If anything, a worm will slow down a computer or network by sucking up hardware resources or internet bandwidth (again, similar to a real parasite).

But some worms carry malicious payloads—code that makes your computer vulnerable to other malware. Since worms can quietly (and harmlessly) duplicate themselves across networks, they make great vehicles for large-scale virus attacks or ransomware attacks on governments and businesses.

Modern Internet Worms Usually Carry Payloads

On their own, worms are mostly harmless. Sure, they slow down computers and turn high-speed networks into snails, but when compared with file-corrupting viruses and hundred-thousand-dollar ransomware, worms are a walk in the park. That is unless the worm carries a payload.



GaudiLab/Shutterstock

As of right now, hackers rarely create payload-less worms. Remember, worms target system vulnerabilities. In the age of frustratingly frequent software updates, those vulnerabilities change week by week. Additionally, when a hacker spreads a worm, they're effectively telling tech companies that an OS vulnerability exists. Once tech companies detect that worm through in-house testing or reports from anti-virus companies, they'll respond by patching the vulnerability that made the worm possible.

So instead of wasting a perfectly good system vulnerability on a crappy worm, modern hackers like to focus their efforts on large-scale payload attacks. The 2004 Mydoom worm, as an example, contained a RAT payload, which allowed hackers to access infected

computers remotely. Since worms travel across networks, these hackers gained access to a ton of different computers, and they used this access to perform a DDOS attack on the SCO Group website.

In the past, when system vulnerabilities were common, and updates came infrequently, payload-less worms were prevalent. These worms were easy to create, fun for novice hackers to deploy, and they usually just slowed down computers to frustrate average users. And while some of these worms, like the Morris worm, were created to raise awareness about software vulnerabilities, they still had the unintended effect of slowing down computers.

Worms Are Easy to Avoid

In theory, worms should be harder to avoid than most other malware. Worms can travel over a network without your knowledge, while viruses and trojans have to be manually downloaded onto a computer. But because of frequent system updates and built-in anti-virus software, you don't have to worry too much about worms. Just keep your OS and your anti-virus up to date (enable auto-updates), and you should be fine. If you're still using Windows XP, you might be in trouble!

Microsoft

That being said, you can pick up a worm through a software download, or even by opening an infected email attachment. If you want to protect yourself from any malware (including worms), then don't download files or open email attachments from sources that you don't trust.

RELATED: ***Still on Windows XP? Update Manually or Get Wormed***

Use Anti-Virus to Protect and De-Worm Your Computer

There's a good chance that your computer is worm-free, even if it's running a bit slow. That being said, it never hurts to run good antivirus software.

Windows PCs come with reliable anti-virus software called Windows Defender. It can automatically scan your PC for viruses, but it's worth running a manual scan if you want some peace of mind. If you want to bring out the big de-worming guns, then try a 3rd party anti-virus software, like Kaspersky or Malwarebytes. These programs are used and trusted by businesses, and they're sure to find any worms that are too sneaky for Windows Defender.

Sure, hackers can create malware that slips past anti-virus software. But hackers rarely waste that malware on small fries. Super sneaky worms with dangerous payloads are usually reserved for large corporations, governments, and multi-millionaires. If your anti-virus doesn't find a worm, then you're probably worm-free.

RELATED: ***10 Quick Ways to Speed Up a Slow PC Running Windows 7, 8, or 10***