Electronic Design

WILLIAM WONG | Technology Editor

What's the Difference Between Ransomware and Malware?

The number of systems being attacked using ransomware is on the rise. But is there a difference between ransomware and malware?

As evidenced by a worldwide attack on hospital and industrial systems that's currently getting a lot of press, the number of systems being attacked using ransomware is on the rise. The attack in question uses the WannaCrypt ransomware based on WannaCry. And it brings up a good question: Is there a difference between ransomware and malware?

Simply put, ransomware is a subset of malware. Malware attacks usually come in the form of a computer virus or worm. A virus piggybacks on something like a document, spreadsheet or e-mail, whereas a worm is a more active attack. It starts on a networked computer system and attempts to subvert one or more computers on the network. This used to be difficult when networked computers were limited in number and connectivity. These days, of course, the internet effectively links billions of devices.

Present-day malware typically consists of a combination of one or more viruses and worms. This allows the malware to remain hidden and spread itself among files on a host computer, as well as spreading to other computers. Malware tends to be specific to a platform like Windows, or even an application. This allows the malware to target specific security holes or improperly configured systems.

Ransomware differs primarily in its approach after a successful attack. Non-ransomware malware may simply be annoying or slightly malicious, deleting files or changing the system configuration (e.g, a screen background). More malicious malware may reformat a disk or corrupt files on the system. It may also remain hidden and communicate with a control system so it can be part of a distributed denial of service (DDOS) attack. In addition, malware may try to capture information from passwords and keystrokes to documents, and then forward this information to a control system.

Ransomware comes into play when the malware notifies the system's user that it has been attacked, but after it has done something to the computer such as encrypt the disk or files. The notification normally demands some sort of payment to restore the computer to its prior state.

In theory, the attacker who manages the ransomware will remotely readjust the computer once payment has been made. Of course, just like in a traditional ransom situation, they may not.

Following the money is how a conventional ransom attack is often traced back to the perpetrator. Doing so is a bit more difficult these days, however, as most ransomware attackers now ask for payment using cypto currencies like Bitcoin *(see "What's the Difference Between Blockchains, Cryptocurrency, Audit Trails, and Databases?" on electronicdesign.com)*. Delivery often takes place through a communication system that keeps users anonymous.

The WannaCrypt attack encrypted files on a Windows computer and then demands a ransom payment of $300 in Bitcoins. If this is not done within three days of the initial attack, the amount is increased to $600. This ransomware deletes files on the infected machine if this continues past a week.

WannaCrypt subverts Windows machines using a bug in the Server Message Block (SMB) protocol. Microsoft issued the MS-17-010 security patch on March 14th to address the problem, but systems need to install this update to be protected. Typically WannaCrypt needs to arrive via other means since most SMB networks will be behind a firewall/gateway. Of course, improperly configured computers attached directly to the internet would be susceptible as well.

WannaCrypt is just one example of ransomware, albeit a notable one that has affected tens of thousands of computers (primarily in Europe, although it reach is worldwide). Also of note is that it asks for small amounts of money, and has a kill switch—the latter was discovered by a researcher; otherwise it

may have spread wider that it already has.

One way to recover from this type of ransomware attack is to resort to backups, if they exist. Unfortunately, many do not have backups that are isolated from the host computer. Backups stored on a disk attacked to a compromised computer would be under attack, as well.

Ransomware should be of particular concern to embedded developers, since this type of attack is not limited to workstations or servers. In fact, many embedded systems already run Windows. Embedded systems often have additional challenges because the update process may be restricted due to one or more considerations. For example, medical systems often require certification that prevents arbitrary updates to be applied. Many of the attack vectors for these systems are often discovered after these restrictions are put in place.

Developers need to be aware that small ransoms like that associated with WannaCrypt are only the beginning. Compromising hundreds of expensive devices or millions of inexpensive devices via ransomware can result in significant ransoms from companies that sell or manage such a large collection. It is even possible to only notify the company associated with these compromised devices while keeping the owners of the devices in the dark.

Still, preventing ransomware attacks is no different than preventing security breaches in general. It means implementing proper security measures as well as minimizing bugs—or, hopefully, eliminating them all. Remote updates can help assuming fixes can be deployed before bugs can be exploited.

One final note: Keep in mind that WannaCrypt works even if the system employs secure boot. This is because the problem occurs in the secured software.