Situation Update

On May 12, 2017 there were multiple public reports of an ongoing large-scale cyberattack involving a variant of the ransomware named WannaCry (aka WCry). These attacks are targeting and have affected users from various countries across the globe.

The WannaCry threat will encrypt data files on infected computers and ask users to pay a $300 US ransom in bitcoin to decrypt their files. The ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, the encrypted files will be deleted.

Analysis indicates the attack spreads through an SMB remote code execution in Microsoft Windows announced and patched by Microsoft on March 14, 2017. Users who have installed this patch are not susceptible. A specific exploit against this vulnerability, code-named "Eternal Blue", and was made available through a dump of various attack tools by the group Shadow Brokers, on April 14, 2017.

Symantec has had generic protection against this vulnerability through our Intrusion Prevention System (IPS) network protection technology in Symantec Endpoint Protection (SEP) and Norton products prior to the release of the WannaCry attacks.

What protections does Symantec provide for our endpoint customers?

There are two basic ways that customers can be protected against this threat:

1. Customers who have installed the Windows security update MS17-010 are not vulnerable to this threat. Symantec Endpoint Management can be leveraged to efficiently distribute this and other patches and software updates across the enterprise.

2. Symantec and Norton products provide a range of protection against this threat on systems that have not installed the patch:

    a. All SEP 14, SEP 12, SEP SBE, and SEP Cloud customers already have protection that prevents the spread of WannaCry via SMB, through our network Intrusion Prevention System (IPS) network protection technology.
    b. There is protection to block the operation of all known variants of the ransomware for SEP 14, SEP 12, SEP SBE, and SEP Cloud customers via our latest available signature updates. We have signatures released as early as March 31, 2017 that block at least one variant of WannaCry.

c. SEP 14, SEP Cloud, and SEP SBE hosted edition customers also have additional advanced protection capabilities from the operation of the threat once installed on a given computer. Our advanced machine learning technology proactively detected many of the WannaCry variants at the time of their release. And the Intelligent Threat Cloud feature will also immediately provide protection against new variants of WannaCry. ***Note:*** Intelligent Threat Cloud feature is enabled ("on") by default, and we recommend that customers assure it remains enabled in their environments.

We also recommend that customers assure that SEP's Insight reputation-based technology and SONAR behavioral technology are enabled. Both can provide additional proactive protection capabilities for new versions of WannaCry.

Are Symantec Proxy customers protected?

Because we have real-time sharing of Symantec and Blue Coat intelligence, all WannaCry samples blocked by SEP will also be automatically be blocked for Blue Customers who have our Content Analysis System (CAS). Note that this capability is not available in the older ProxyAV predecessor to Content Analysis System, although ProxyAV's malware scanning engines may independently be able to block WannaCry. As additional samples are discovered by Symantec, appropriate protection will automatically be added for both SEP and Blue Coat proxy customers.

Are Symantec email customers protected?

All Symantec email customers are fully protected from WannaCry with our latest released set of signatures. Our Skeptic and Link Following technologies available in our Email Security.cloud product will provide additional proactive protections.

Summary

It is highly recommended that all customers keep their software (SEP 14, ProxySG, MS Patches, etc.) up to date on the latest versions to mitigate the risk of future infections.

Resources

- WannaCry Variant Alert Article
- Symantec Official Blog: *What You Need to Know about the WannaCry Ransomware*
- Contact Symantec Support *(select the appropriate country)*

Technical Details

Review Symantec's complete write-up on the WannaCry ransomware threat for technical details.

A pre-recorded webcast will be available to customers and partners on Monday, 15 May, on the Symantec Official Blog.