# *WannaCry* Ransomware Campaign Update

## Executive Summary

As you are likely aware, a highly prolific WannaCry ransomware campaign has been impacting organizations globally since May 12, 2017. WannaCry (or WCry or WanaCryptor) malware is a self-propagating (worm-like) ransomware that spreads through internal networks and over the Internet. FireEye is continuing to investigate this threat as it evolves, but we also want to provide our customers with current information on what we know about this campaign, as well as provide access to resources that will be constantly updated as we learn more about it.

Based on our current knowledge, WannaCry spreads internally within organizations by exploiting what is being referred to as EternalBlue. This is a vulnerability in the Microsoft Server Message Block (SMB) protocol, a network sharing protocol that enables the sharing of files between networked Windows-based computers. The SMB vulnerability is the only propagation method that we have confirmed at this time.

FireEye products can detect attacks at the network perimeter that originate over web or email attack vectors, however, we are not positioned to block exploitation of the SMB vulnerability that occurs between Windows machines internal to the network. A patch for the vulnerability was issued by Microsoft in March 2017, and FireEye recommends following and monitoring Microsoft's customer guidance.

FireEye's Network, Email, and Endpoint products have ransomware detection capabilities that can detect and, if deployed in-line, block, web and email distributed ransomware. FireEye products also detect later stage activity, such as command-and-control communications and can use indicators to detect existing WannaCry infections.

Since a single infection can allow this malware to spread to all vulnerable and accessible systems within the organization, we urge customers to follow Microsoft's guidance for mitigating the SMB vulnerability. Additionally, customers should leverage confirmed indicators to proactively hunt for possible infections and quarantine infected systems. These indicators have been deployed to FireEye Endpoint Security (HX Series) customers. More details on the intelligence we have gathered on the threat have been shared with our FireEye as a Service and iSIGHT Intelligence customers. Due to the unprecedented nature of this threat, we are making this available in the FireEye Support Community (login required).

Intelligence activities are ongoing, and product and service detection, hunting and alerting capabilities are being continuously enhanced as we learn more about this threat. FireEye encourages you to visit our blog which will be updated on a regular basis. A blog post is available now and will be updated with indicators of compromise as we confirm and validate them.

In addition, FireEye has also scheduled two identical webinars on Tuesday, May 16, 2017, to discuss this threat and answer questions. You can register for these webinars by following the links below:

NAM/EMEA:
https://www2.fireeye.com/WBNR_Wanna_Cry_Threat_Details_and_Risk_Management.html

APAC:
https://www2.fireeye.com/WBNR_Wanna_Cry_Threat_Details_and_Risk_Management_APAC.html

## FireEye Security Best Practices

FireEye recommends the following security best practices:

- Always keep the product version up-to-date and maintain default automated Security Content update configuration setting
- Limit network access to the management interface(s) of the appliance with firewalls or similar measures
- Only issue accounts to trusted administrators
- Utilize strong passwords
- Monitor logs
- Restrict physical access to the appliance to trusted administrators

If you have any questions, please contact FireEye Support at support@fireeye.com or 877 347-3393 (877-FIREEYE) or 408 321-6300.

To report vulnerabilities in FireEye products, please email security@FireEye.com.