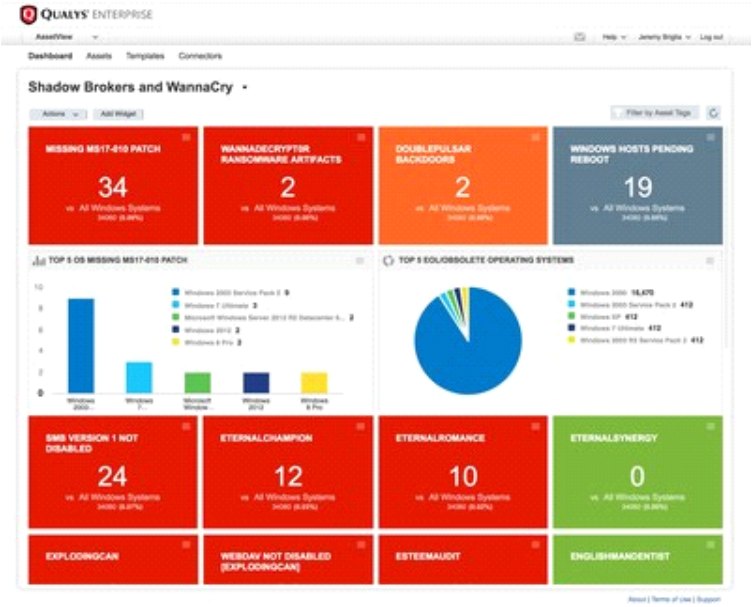
May 19, 2017

# Security Alert: Qualys Offers 30-Day Free Unlimited Service to Identify and Track Remediation of Assets Exploitable by WannaCry Ransomware

REDWOOD CITY, Calif., May 19, 2017 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of cloud-based security and compliance solutions, today announced that it is offering businesses worldwide 30 days of free service that will allow them to identify, track and remediate assets at risk to the WannaCry ransomware virus that has impacted hundreds of thousands of computers around the world. The offer is available at qualys.com/wannacry-30days.




This malware, which utilizes the ETERNALBLUE exploit against the MS17-010 vulnerability, encrypts files and demands a ransom payment to decrypt them. Enterprises face the daunting task of determining where this vulnerability exists within their global IT environments, and existing enterprise security solutions are slow to deploy. In response to this attack, Qualys is offering customers worldwide unlimited comprehensive scanning capabilities via its cloud-based platform that can be deployed immediately. This service helps enterprises to detect, track and remediate WannaCry and its variants across global IT assets. It also offers reports and a dashboard to visualize the impact on assets in real-time and track remediation efforts, giving chief information security officers the continuous visibility they need to contain this critical threat.

**Qualys signature detections to WannaCry include the following Qualys IDs (QIDs):**

- QID 91345 - Microsoft Server Message Block (SMB) Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers
  Qualys initiated coverage for this missing patch on supported platforms on March 14, a month before the Shadow Brokers dump. This QID has been updated to also detect the new patches for End-of-Life (EOL) versions of Windows.
- QID 91360 - Microsoft Windows SMBv1 and NetBIOS over TCP/IP (NBT) Remote Code Execution - Shadow Brokers (ETERNALBLUE) MS17-010
  Qualys added this QID immediately following the Shadow Brokers release on April 14 to also detect the vulnerability exploited by ETERNALBLUE across all Windows platforms. This QID has also been updated to not flag if the EOL patches have been installed.
- QID 70077 - Double Pulsar Backdoor Detected (Shadow Brokers)
  Detects the presence of the DOUBLEPULSAR backdoor that WannaCry can leverage to propagate.
- QID 1029 - WannaCrypt Ransomware Detected. Detects WannaCry and can be used to trigger alerts on new infections.

**Qualys' 30-day unlimited free offer includes:**

- **Vulnerability Management** - Provides comprehensive scanning capabilities through network scanners or via cloud

agents so organizations can quickly and accurately identify which assets are vulnerable or have been infected with WannaCry.

- **ThreatPROTECT** - Provides one-click access to a dashboard of impacted assets through the Live Threat Intelligence Feed that provides most-up-to-date threats, as well as a detailed analysis of ETERNALBLUE and WannaCry.
- **AssetView** - Can help organizations locate and track legacy and current Windows assets impacted by these exploits in dynamic widgets.
- **Continuous Monitoring** - Allows organizations to create alerts to track any WannaCry infections that pop up on their network.
- **Scanning of unlimited IP addresses**
- **Deployment of unlimited Virtual Scanner Appliances or Cloud Agents**

**Additional Resources:**

- WannaCry up-to-date blog post: qualys.com/wannacry
- Follow Qualys on LinkedIn and Twitter
- Read more about the Qualys Cloud Platform

**About Qualys**
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL Technologies, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon, and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.



**QUALYS MEDIA CONTACT**
David Conner
Qualys, Inc.
dconner@qualys.com
650-801-6196

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/security-alert-qualys-offers-30-day-free-unlimited-service-to-identify-and-track-remediation-of-assets-exploitable-by-wannacry-ransomware-300460559.html

SOURCE Qualys, Inc.

News Provided by Acquire Media