THREAT BRIEF

Gartner
COOL VENDOR
2020™

BlueKeep (CVE-2019-0708)

Detecting a Remote Desktop Protocol Exploit • Summer 2019

BlueKeep is a vulnerability in Microsoft's Remote Desktop Protocol (RDP) discovered by the UK's National Cyber Security Centre. This vulnerability affects RDP installations on Windows 7 and below unless BlueKeep-specific patches have been applied. This allows attackers to bypass access restrictions and communicate with a server as a remote terminal. Initial proofs of concept demonstrating the threat represented by BlueKeep were released publicly on platforms such as GitHub, and a BlueKeep module was incorporated into the Metasploit toolkit.

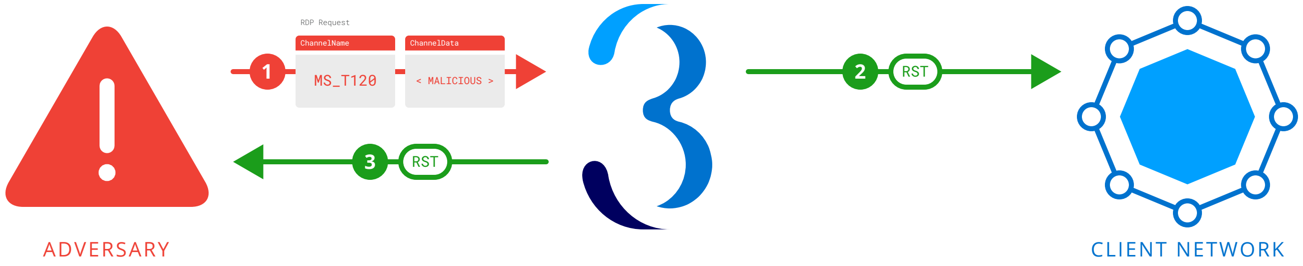
Ultimately, BlueKeep exploits have grown in scope and have been discovered in the wild as part of active malware campaigns delivering cryptocurrency miners, which slow the performance of a system or network. BlueKeep's potential for harm goes far beyond cryptocurrency mining, however. BlueKeep infiltration of a network permits installation of any form of malware, including ransomware. As an unauthenticated remote exploit, BlueKeep has the potential to cause wide-ranging and devastating harm.

Neutralizing the Vulnerability

Trinity Cyber detects BlueKeep by identifying inbound RDP request traffic with the distinct ChannelName of "MS_T120" within the ClientNetworkData section of the request. Our methodology bidirectionally detects both the presence of a BlueKeep exploit and, in the case of scanning activity, detects and correlates the outbound RDP server response indicating a vulnerable machine.

When we detect a BlueKeep exploit or scanning activity, we immediately take one of several customizable actions on behalf of a client to prevent the attack. By default, we transparently close the attacker's session or change the response from a vulnerable machine to appear as if the machine is not vulnerable.

Trinity Cyber's unique actions protect our clients by preventing threat actors from using the BlueKeep vulnerability to gain unrestricted access to deliver malware onto their network. Period.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

© 2020 Trinity Cyber, Inc. CONFIDENTIAL AND PROPRIETARY

Trinity Cyber was named a Cool Vendor in Gartner's Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., 30 September 2020.

The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Trinity Cyber