ERT Threat Alert

Coronavirus: Recommendations To Keep Critical Services Available

March 18, 2020

To control the spread of the coronavirus (COVID-19), many organizations are requesting employees to work remotely. Doing so means leveraging enterprise virtual private networks (VPNs) and remote desktop solutions to connect to services. This shift opens the door to an array of cybersecurity threats that specifically target these networks and solutions. Protecting these tools requires implementation of specific steps to ensure business continuity during this global pandemic.

Recommendations to Protect Against Service Disruption

Organizations must take preventive measures to ensure service continuity as they increasingly depend on remote access for day-to-day operations. Exposing critical services on the internet makes them vulnerable to service disruption by DoS/DDoS attacks. To keep critical services available, Radware recommends:

- Implementing a hybrid DDoS solution that combines both cloud-based DDoS with on-premise DDoS protection to provide the best attack coverage while minimizing latency
- Ensure your DDoS mitigation solution can both protect legitimate traffic and handle any expected growth as more employees work remotely. Add additional capacity if needed
- Select solutions that provide behavioral-based protection from all types of attacks, including burst attacks, DNS-based attacks and encryption-based attacks

Recommendations to Protect Against VPN Vulnerabilities

Remote access solutions have become increasingly vulnerable over the past 12 months. Both U.S. and U.K. government agencies have issued multiple warnings over the previous year as enterprise VPNs have become the attack vector of choice for advanced persistent threat (APT) actors. Radware recommends:

- Updating VPNs, network infrastructure devices and devices used to remote into work environments with the latest software patches
- Implement multi-factor authentication (MFA) on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords and not reuse passwords for other purposes or sites
- Reset credentials associated with potentially affected VPNs
- Implement granular access controls in VPN solutions to limit the access based on user profiles
- Ensure and enforce the security posture of client devices before allowing access to internal resources

Recommendations to Protect Against the BlueKeep RDP Vulnerability

Microsoft's remote desktop solution, based on the remote desktop protocol (RDP), was the subject of numerous National Security Agency warnings based on research that revealed that approximately one million internet-facing machines were vulnerable to a vulnerability named BlueKeep. According to research conducted by Coveware, RDP was the attack vector used by every two out of three ransomwares.

Microsoft provided updates in May of 2019. A list of security updates and knowledgebase articles for impacted windows systems is available from Microsoft.

Radware DefensePro customers have a specific signature that protects from known BlueKeep attacks as part of their Security Update Signature subscription. The signature is referenced as RWID 18944: RDP-MS-T120-CHANNEL-VER1-RCE (CVE-2019-0708).

Recommendations to Protect Against RDP Account Takeover Attacks

Approximately 0.08% of RDP Brute Force attacks are successful. Brute Force attacks typically last two to three days, according to a recent Microsoft report. To protect against account takeover attacks:

- Microsoft recommends that system administrators combine and monitor multiple signals for detecting RDP inbound brute force traffic on their servers.
- Radware's ERT Active Attacker Feed provides proactive protection against scans and attacks from most malicious devices and servers recorded in Radware's global deception network, allowing organizations to focus on malicious traffic.
- Radware recommends leveraging traffic filters on DefensePro to limit the number of new sessions to the RDP services.

Recommendations to Protect Against Phishing Attacks

Fear and the need for information provides an opportunity for cyber scams and abuses. Numerous phishing campaigns have been discovered since the coronavirus pandemic. Stay current with anti-malware and phishing products and inform employees about the dangers of opening attachments or clicking links in emails from untrusted sources. Inform employees about an expected increase in phishing attempts that promise information about COVID-19.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.