Dragon Advance Tech

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

Cybersecurity Alert: Remote Desktop Protocol (RDP) Remote Code Execution

TLP:GREEN

Hong Kong SMEs' Internet-facing RDP services are vulnerable to advanced attacks
After collecting sufficient data, attackers may plant ransomware into the compromised systems

The Computer Security Incident Response Team from Dragon Advance Tech is aware of the trend of ransomware incidents in Hong Kong. Since 2017, more than 20 attacks by a ransomware called "Crysis" have been identified in Hong Kong. This kind of RDP brute force is still a popular approach to gain access into a system. The attackers have used similar tactics, techniques, and procedures (TTPs) to compromise a system. However, our incident response team has discovered that attackers may use some advanced attacking tools "in the wild"—meaning threats spreading among real world computers, as opposed to test systems—to compromise a system. The old Microsoft Windows 2003 or Windows XP systems are most vulnerable to attack.

Systems Affected

Microsoft Windows Server 2003, Microsoft Windows XP

Description

Many SMEs in Hong Kong outsource their IT support to a third-party IT service provider. Usually, the third-party IT support may ask the SME to open the port 3389, RDP service, in the firewall/router for their remote support use. It is convenient for IT support, but it also exposes the RDP internal machine to the Internet.

The previous Crysis ransomware cases were all related to unauthorized access via RDP, and there were traces of RDP brute forcing. However, we discovered a different case recently: We found only one successful RDP login from a foreign IP address, and we could not identify any traces of RDP brute force. The ransomware was planted and executed about an hour after the successful RDP login.

Technical Details

The security analysts of Dragon Advance Tech performed further investigation on the victim's machine and identified one possible reason. The victim machine appears to be vulnerable to the CVE-2017-0176 Remote Buffer Overflow Vulnerability.[i]

The infected machine was running Windows Server 2003, for which Microsoft had discontinued support since 2015. The machine was a domain controller, and the RDP smart card authentication was enabled. These were conditions that enabled the exploit.

Attackers can easily obtain a tool in the wild to exploit this vulnerability. The WannaCry Ransomware was using the "EternalBlue" exploit. The "EternalBlue" was a notorious exploit that originated from the Equation Group. There is another exploitation tool from the infamous leaks from the Equation Group called "EsteemAudit", which targets RDP vulnerability.[ii] This hacking tool allows attackers to stealthily bypass system authentication and gain kernel mode code execution, which means attackers can execute instructions at the highest privilege in the system; basically, he can do whatever he wants. Hence, password and data exfiltration are possible. The research team of Dragon Advance Tech has reconstructed the same environment to simulate the attack and confirmed that the hacking tool works on Windows Server 2003 and Windows XP.

We cannot positively confirm the actor, even though we found the hacking IP was originated from the UK, and that an advanced hacking tool was used because it is stealthy. We could not find a lot of digital traces in the infected machine, except that a ransomware was planted. We believe that the Windows systems with discontinued support and open RDP service to the Internet may have been subject to either advanced hacking tool attacks or brute force attacks. Up to the time of writing, we found 63 Window Server 2003/XP hosts with Internet-facing RDP in Hong Kong (see Shodan report link on 24/2/2019).

Mitigation

If your Windows systems are running any of the above-mentioned versions and they are opened with port 3389, disable it unless it is necessary and disable the smart card authentication module in the Group Policy or in the registry.
For registry, set the key "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\EnableSmartCard" to 0. If you are not sure if any of your machines are exposed to the Internet, please consult your IT support.

"IT CAN HAPPEN TO ANYONE AND MAY HAPPEN AGAIN"

[i] Remote desktop protocol remote code execution vulnerability https://support.microsoft.com/en-us/help/4022747/security-update-for-windows-xp-and-windows-server-2003

[ii] A Dissection of the "EsteemAudit" Windows Remote Desktop Exploit https://unit42.paloaltonetworks.com/unit42-dissection-esteemaudit-windows-remote-desktop-exploit/