HC3 Intelligence Briefing
Remote Desktop Protocol
Exploitation
OVERALL CLASSIFICATION IS
TLP:WHITE

November 21, 2019
Agenda

• Overview
• History
• Usage
• Maturity of RDP implementation
• Why does RDP matter to healthcare cybersecurity?
• RDP Exploitation
• Major exploits: Bluekeep and DejaBlue
• RDP Threats – who and what attacks RDP?
• Securing RDP
• References
• Questions

Slides Key:

- Non-Technical: managerial, strategic and high-level (general audience)
- Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Overview

- Proprietary protocol, originally developed by Microsoft
- Formerly known as Terminal Services Client
  - Introduced in Windows NT 4.0 (1996)
  - Became part of Remote Desktop Services (RDS) in 2009
- Implementations currently exist for Windows, Unix, Linux, Mac, iOS and Android, etc…
- Legitimate use for remote access for IT support:
  - Administration
  - Maintenance
  - Troubleshooting
  - User assistance
- Utilizes TCP and UDP ports 3389 by default
- Highly vulnerable to attack
  - Remote access is desired by hackers
- Frequently exploited by many vulnerabilities and tactics
## The evolution of RDP:

<table>
<thead>
<tr>
<th>RDP VERSION</th>
<th>WINDOWS OS</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Win NT 4.0</td>
<td>First version of RDP, Based on the ITU-T T.128 application sharing protocol; introduced with terminal services</td>
</tr>
<tr>
<td>5</td>
<td>Win 2000 Server</td>
<td>Support for printing; improved bandwidth usage</td>
</tr>
<tr>
<td>5.1</td>
<td>Windows XP</td>
<td>Support for 24-bit color and sound; Client available for Windows 2000, Windows 95/98 and Windows NT 4.0.; Name of the client changed from Terminal Services Client to Remote Desktop Connection</td>
</tr>
<tr>
<td>5.2</td>
<td>Windows server 2003</td>
<td>Support for console mode connections, session directory, and local resource mapping; Transport Layer Security (TLS) available for authentication and encryption with server</td>
</tr>
<tr>
<td>6</td>
<td>Windows Vista</td>
<td>Multi-monitor spanning and large desktop support</td>
</tr>
<tr>
<td>6.1</td>
<td>Windows Server 2008, Windows Vista Service Pack 1, Windows XP Service Pack 3</td>
<td>Support for connecting remotely to individual programs</td>
</tr>
<tr>
<td>7</td>
<td>Windows Server 2007 R2, Windows 7</td>
<td>Renamed Terminal Services to Remote Desktop Services</td>
</tr>
<tr>
<td>7.1</td>
<td>Windows 7 Service Pack 1, Windows 2008 R2 Service Pack 1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Windows 8, Windows Server 2012</td>
<td>Automatic selection of TCP or UD; Adaptive Graphics; multi touch support</td>
</tr>
<tr>
<td>8.1</td>
<td>Windows 8.1, Windows Server 2012 R2</td>
<td>Support for session shadowing</td>
</tr>
</tbody>
</table>
Usage

- Most current RDP implementations allow for:
  - Windows Presentation Foundation (WPF) applications and remoting
  - Clipboard sharing between a remote server and a local client
  - Remote desktop applications execution on client machines
  - Aeroglass remoting
  - Windows Media Player (WMP) redirection
  - Implementation on non-Microsoft platforms
    - e.g. Unix/Linux platforms use rdesktop
  - Mouse and user keyboard data encryption
  - Audio, printer, port and file redirection
  - Multiple monitor support

Image courtesy of Microsoft.com
Maturity of RDP implementation

Windows Server 2008 R2: Remote Desktop Services Component Architecture

Image courtesy of Microsoft.com
Why does RDP matter to healthcare cybersecurity?

- Targeting
  - ECRI Institute’s annual Top 10 Health Technology Hazards for 2019
    - Hackers attacking healthcare through remote access systems and disrupting operations is the number one patient safety risk
  - Oleg Kolesnikov, Head of Securonix Threat Research Labs, Referring to RDP:
    - “…if it’s targeted, particularly in healthcare, and exploited, the results can be much more severe…”
  - Trapx Security:
    - “One of the most common breach scenarios, whether by an insider (a rogue employee) or by an external attacker who has successfully breached the perimeter, happens through RDP.”

Remote Access System Hacking Is No. 1 Patient Safety Risk

Hackers attacking healthcare through remote access systems and disrupting operations is the number one patient safety risk.
RDP exploitation

• Sophos leveraged Shodan to assess global RDP vulnerabilities:

RDP is already being abused, every day, to devastating effect. - Sophos
RDP exploitation (continued)

- FBI released RDP PSA in September 2018:
  - “…as an attack vector on the rise since mid-late 2016…”
  - Frequently for sale on the dark web
  - Used to:
    - Compromise identities
    - Steal login credentials
    - Demand ransom (ransomware)
    - Steal other sensitive information
  - Vulnerabilities:
    - Weak passwords
    - Outdated installations
    - Unrestricted RDP access
    - Unlimited authentication attempts

- Threats: CrySiS, CryptON, Samsam
- Defense: Auditing, 2FA, logging, etc…
Major exploits: Bluekeep and DejaBlue

- BlueKeep (and related vulnerabilities)
  - Target Microsoft Windows
    - Windows XP
    - Windows Server 2003
    - Windows Vista
    - Windows 7
    - Windows Server 2008
    - Windows 10
  - CVE-2019-0708 (Bluekeep)
    - CVE-2019-1181, CVE-2019-1182 (DejaBlue)
  - Remote Code execution
  - “Wormable”
  - Microsoft Bluekeep severity categorization: Critical
  - Microsoft released patch for Bluekeep in May of 2019, DejaBlue in Oct. 2019
    - Two weeks after Bluekeep patch was released, one researcher noted almost 1M systems still remained unpatched
  - NSA released Bluekeep warning
Major exploits: Bluekeep and DejaBlue (continued)

- Microsoft and NSA Bluekeep releases:

A Reminder to Update Your Systems to Prevent a Worm

On May 14, Microsoft released fixes for a critical Remote Code Execution vulnerability, CVE-2019-0708, in Remote Desktop Services — formerly known as Terminal Services — that affects some older versions of Windows. In our previous blog post on this topic we warned that the vulnerability is "wormable," and that future malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017.

Microsoft is confident that an exploit exists for this vulnerability, and if recent reports are accurate, nearly one million computers connected directly to the Internet are still vulnerable to CVE-2019-0708. Many more within corporate networks may also be vulnerable. It only takes one vulnerable computer connected to the Internet to provide a potential gateway into these corporate networks, where advanced malware could spread, infecting computers across the enterprise. This scenario could be even worse for those who have not kept their internal systems updated with the latest fixes, as any future malware may also attempt further exploitation of vulnerabilities that have already been fixed.

It's been only two weeks since the fix was released and there has been no sign of a worm yet. This does not mean that we're out of the woods. If we look at the events leading up to the start of the WannaCry attacks, they serve to inform the risks of not applying fixes for this vulnerability in a timely manner.

Our recommendation remains the same. We strongly advise that all affected systems should be updated as soon as possible.

It is possible that we won’t see this vulnerability incorporated into malware.

But that's not the way to bet.
## RDP Threats – who and what attacks RDP?

### Ransomware
- Apocalypse
- CrySiS/Dharma
- CryptON
- Samsam (Samas)
- Ryuk
- Sodinokibi
- SynAck
- DMA Locker
- LockCrypt
- Scarabey
- Horsuke
- Bit Paymer
- RSAUtil
- Xpan
- LowLevel
- Smrss32
- WannaCry
- Aura/BandarChor
- ACCDFISA
- Globe
- And more…

### Threat Actors
- APT1
- APT3
- APT39
- APT41
- Axiom
- Carbanak
- Cobalt Group
- Cobalt Strike
- DarkComet
- Dragonfly 2.0
- FIN10
- FIN6
- FIN8
- jRAT
- Koadic
- Lazarus Group
- Leviathan
- menuPass
- njRAT
- OilRig
- Patchwork
- Pupy
- QuasarRAT
- Revenge RAT
- ServHelper
- Stolen Pencil
- TEMP.Veles
- zwShell/ZxShell
- And more…
Securing RDP

- Recommended cybersecurity defense and response practices:
Securing RDP (continued)

• Specific steps for securing RDP
  • Whenever possible on Windows implementation, use group policy object (GPO) functionality to centrally manage RDP [3.S.A], [3.L.B]
  • Use strong/complex passwords; require periodic password changes [3.S.A], [3.M.C], [3.L.C]
    • Letters, numbers, symbols and password length minimums
    • Balance between password change window that is too long and too short
    • Filter via IP address, MAC address, etc…
  • Reassign RDP to another port (change listening port from default 3389) [6.M.A]
  • Update software; Apply patches [7.S.A], [7.M.D]
    • Patch management program

RDP Stands for “Really DO Patch!”

McAfee.com
Securing RDP (continued)

• Specific steps for securing RDP (continued)
  • Use RDP gateway [6.S.A], [6.M.B], [6.L.A]
    • Funnell remote connections through a single “gateway” server
  • Tunnel Remote Desktop connections through IPSec or SSH [4.S.A], [4.M.C], [4.L.A]
    • Alternate to RDP gateway
  • Set restrictions on accounts [3.S.A], [3.M.A], [3.L.C]
    • Enable network-level authentication
      • Additional layer of authentication
    • Implement two-factor authentication
    • Limit RDP usage to only those whose role absolutely requires it
    • Implement RDP account lockout policy
    • Implement auto-disable for accounts that are not used after set period of time
  • Log and review all RDP access
    • On Windows system, domain controller can audit
    • Firewall logs
References


• Camp, Cameron, Remote Desktop (RDP) Hacking 101: I can see your desktop from here!, ESET - We Live Security, 9/16/2013, https://www.welivesecurity.com/2013/09/16/remote-desktop-rdp-hacking-101-i-can-see-your-desktop-from-here/

• Definition of: Terminal Services, PC Mag Encyclopedia, https://www.pcmag.com/encyclopedia/term/52755/terminal-services


References (continued)

References (continued)

Questions

Upcoming Briefs

• Bluekeep
• Incident Response

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.