Agenda

- What is BlueKeep
- Timeline of BlueKeep
- BlueKeep Today
- Initial Attempts to Exploit BlueKeep
- Why Initial Attempts Failed
- BlueKeep Tomorrow
- Mitigations
- Indicators of Compromise (IOCs)
- HC3 Contact Information
- References

Slides Key:

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

- BlueKeep (CVE-2019-0708)
  - Vulnerability in Microsoft’s (MS) Remote Desktop Protocol
    - Grants hackers full remote access and code execution on unpatched machines
      - No user interaction required
      - Essential owns the machine, malicious actor can do as they please
      - Deja Blue (Related BlueKeep Vulnerabilities) affects: Windows 8, 10, and all older windows versions
      - EternalBlue affects: Server Message Block version 1 (SMBv1)
    - “Wormable” meaning it has the ability to self propagate (think WannaCry level of damage)
    - MS, NSA, DHS, many other security vendors released advisories and warning on this exploit
**BlueKeep Timeline**

- **2019**
  - **May/14**: Microsoft Released Patch: CVE-2019-0708
  - **Jun/17**: DHS Tested a Working Exploit Against W2000
  - **Jul/23**: 34 Days (Private Exploit)
  - **Jul/24**: 70 Days (Semi-Public Exploit)
  - **Jul/31**: 115 Days (Public Exploit)
  - **Jul/24**: BlueKeep Scanner Discovered in Watchdog Malware
  - **Jul/24**: Significant Uptick in Malicious RDP Activity
  - **Jul/31**: BlueKeep RCE Exploit Module Added to Penetration Testing Tool
  - **Sep/06**: BlueKeep RCE Exploit Module Added to Metasploit
  - **Oct/09**: Metasploit Team Releases BlueKeep Exploit Module
  - **Oct/23**: Coin Miner Exploit BlueKeep Vulnerability
  - **Nov/11**: Tencent
  - **Dec/09**: RiskSense
  - **Dec/23**: Microsoft
  - **Dec/31**: Rapid7

- **2020**
  - **Jan/06**: 148 Days (1st Wild Exploitation Attempt)
  - **Mar/02**: 162 Days (2nd Wild Exploitation Attempt)
  - **May/09**: 34 Days (Private Exploit)
  - **Jun/17**: 70 Days (Semi-Public Exploit)
  - **Jul/24**: 115 Days (Public Exploit)
  - **Jul/24**: BlueKeep Scanner Discovered in Watchdog Malware
  - **Jul/24**: Significant Uptick in Malicious RDP Activity
  - **Jul/31**: BlueKeep RCE Exploit Module Added to Penetration Testing Tool
  - **Sep/06**: BlueKeep RCE Exploit Module Added to Metasploit
  - **Oct/09**: Metasploit Team Releases BlueKeep Exploit Module
  - **Oct/23**: Coin Miner Exploit BlueKeep Vulnerability
  - **Nov/11**: Tencent
  - **Dec/09**: RiskSense
  - **Dec/23**: Microsoft
  - **Dec/31**: Rapid7

- **2021**
  - **Jan/06**: 148 Days (1st Wild Exploitation Attempt)
  - **Mar/02**: 162 Days (2nd Wild Exploitation Attempt)
  - **May/09**: 34 Days (Private Exploit)
  - **Jun/17**: 70 Days (Semi-Public Exploit)
  - **Jul/24**: 115 Days (Public Exploit)
  - **Jul/24**: BlueKeep Scanner Discovered in Watchdog Malware
  - **Jul/24**: Significant Uptick in Malicious RDP Activity
  - **Jul/31**: BlueKeep RCE Exploit Module Added to Penetration Testing Tool
  - **Sep/06**: BlueKeep RCE Exploit Module Added to Metasploit
  - **Oct/09**: Metasploit Team Releases BlueKeep Exploit Module
  - **Oct/23**: Coin Miner Exploit BlueKeep Vulnerability
  - **Nov/11**: Tencent
  - **Dec/09**: RiskSense
  - **Dec/23**: Microsoft
  - **Dec/31**: Rapid7

**Notes**
- Syscall hook removed from BlueKeep payload
- Tencent
- RiskSense
- Microsoft
- Rapid7
Data Covers May 31 to July 2, 2019

“As of July 2, 2019, approximately **805,665 systems** remain online that are vulnerable to BlueKeep, representing a decrease of 17.18% (167,164 systems) compared to May 31.”

“There has been progress made across the board as all industries have demonstrated a reduction in the number of organizations with exposed vulnerable systems since data collected on May 31, 2019, with variable amount of progress made within each industry.” ~BitSight
BlueKeep Today

• Out in the Wild!
  • Don’t panic just yet
  • Spotted by security researchers Kevin Beaumont and Marcus Hutchins in early Nov
    • Beaumont’s honeypots, set up to detect and monitor BlueKeep, kept crashing with “Blue Screen Of Deaths”.
    • Sent Logs to Hutchins for deep dive analysis
• Conclusion
  • No worm function
  • No self propagation
  • Used in low level attacks
    • Done by same group of malicious actors
    • Wild BlueKeep Shellcode matches Metasploits Shellcode
    • Attacks in Sept and Oct shared the same Command and Control infrastructure
      • Attackers most likely using manual port scans to find vulnerable machines
    • Cryptomining attacks ~type of coin is unknown

"They’re not seeking targets. They’re scanning the internet and spraying exploits."

Marcus Hutchins – Kryptos Logic

Side by side of the in-memory shellcode and the metasploit shellcode

Kryptoslogic
## Initial Attempts to Exploit BlueKeep

<table>
<thead>
<tr>
<th>Threat technique or component</th>
<th>Protections</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Scans for vulnerable RDP services</td>
<td>Security update for CVE-2019-0708</td>
</tr>
<tr>
<td>3. Download and execution of multiple obfuscated PowerShell scripts</td>
<td>EDR</td>
</tr>
<tr>
<td>4. Coin miner payload</td>
<td>Windows Defender Antivirus</td>
</tr>
<tr>
<td>5. Scheduled task for payload persistence</td>
<td>EDR</td>
</tr>
<tr>
<td>6. C&amp;C communication</td>
<td>EDR</td>
</tr>
</tbody>
</table>
Why Initial Attempts Failed

• BlueKeep is a **Fussy Exploit**
  • Reason why the attack **failed** was because of an incompatibility between the exploit code and a patch Microsoft had previously issued for the Intel CPU vulnerability known as **Meltdown**
  • Caused many machines to crash, causing many people to discount the potential severity of the BlueKeep vulnerability.
  • Already adapted
    • This incompatibility has already been **fixed** and patched into the Metasploit BlueKeep Module

---

**MalwareTech** @MalwareTechBlog · Nov 2, 2019
Blog post on how I discovered mass exploitation of BlueKeep from a kernel dump of a crashed system. twitter.com/kryptoslogic/s...

**Kryptos Logic** @kryptoslogic
BlueKeep (CVE 2019-0708) exploitation spotted in the wild kryptoslogic.com/blog/2019/11/b...

**Worawit Wang** @sleepya_
From call stack, seems target has kva shadow patch. Original eternalblue kernel shellcode cannot be used on kva shadow patch target. So the exploit failed while running kernel shellcode

12 1:22 AM · Nov 4, 2019
BlueKeep Tomorrow

- Where can BlueKeep go?
  - Will continue to evolve, the risk of this vulnerability can change over time
  - Malicious Actors will focus on efforts that offer the greatest return (money) for effort
    - Wormable feature may used in future attacks
      - Can spread without human interaction
      - Loaded with ransomware or other malicious programs
      - Can cause significant damage (ex. WannaCry)
  - Future attacks may focus supply chain partners
    - Unpatched Servers
    - Managed Service Providers
  - Unpatched systems will remain key in BlueKeep future success
    - Don’t fall into the “Avoidance” (letting an acknowledged risk linger because there is no perceived penalty in procrastinating) trap
BlueKeep Mitigations

- **Patch** and keep the system and its applications updated (or employ virtual patching to legacy or end-of-life systems) [7.S.A], [7.M.D]

- Restrict or **secure** the use of remote desktop services. For example, blocking port 3389 (or disabling it when not in use), can help thwart threats from initiating connections to systems behind the firewall [3.S.A], [3.M.A], [3.L.C]

- Enable network level authentication (NLA) to prevent unauthenticated attackers from exploiting BlueKeep. This can be **configured** in Windows 7 and Windows Server 2008 (including the R2 version) [3.S.A], [3.M.A], [3.L.C]

- Enforce the principle of least privilege. Employing security mechanisms like encryption, lockout policies, and other permission- or role-based access controls provide additional layers of security against attacks or threats that involve compromising remote desktops. [3.S.A], [3.M.A], [3.L.C]
BlueKeep Indicators of Compromise

- **IOCs**
  - IP Addresses
    - 109.176.117.11 port 8000
    - 5.100.251.106 port 52057
    - 217.114.18.50 port 52107
    - 193.27.73.223
    - 217.23.5.20
    - 157.245.82.38
    - 193.104.205.59
    - 217.23.5.70
    - 167.172.224.148
    - 160.20.146.133
    - 138.201.209.190
    - 167.71.240.219
    - 193.104.205.59

- **URLs**
  - hxxp://178.175.141.12:7023/9bccf8cd92/temp
  - hxxp://178.175.141.12:11008/6b53002fb437/temp
  - hxxp://138.201.209.190:10708/cc1ad438c54a/temp

**DoublePulsar**
References

- Microsoft works with researchers to detect and protect against new RDP exploits

- BlueKeep (CVE-2019-0708): From Rumor to Reality

- DejaBlue vs BlueKeep vs Eternal Blue

- Alert (AA19-168A) Microsoft Operating Systems BlueKeep Vulnerability
  https://www.us-cert.gov/ncas/alerts/AA19-168A

- Patch Remote Desktop Services on Legacy Versions of Windows


- CVE-2019-0708
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
References

• Solved: Why in-the-wild Bluekeep exploits are causing patched machines to crash

• Spectre and Meltdown: What you need to know

• BlueKeep: What you Need to Know

• Fixing Remote Windows Kernel Payloads to Bypass Meltdown KVA Shadow
  https://zerosum0x0.blogspot.com/2019/11/fixing-remote-windows-kernel-payloads-meltdown.html

• The First BlueKeep Mass Hacking Is Finally Here—but Don't Panic
  https://www.wired.com/story/bluekeep-hacking-cryptocurrency-mining/

• BlueKeep (CVE 2019-0708) exploitation spotted in the wild

• BlueKeep exploitation activity seen in the wild
  https://doublepulsar.com/bluekeep-exploitation-activity-seen-in-the-wild-bd6ee6e599a6

• Data Insights on the BlueKeep Vulnerability
References

- Avast Business report may help explain why users are resisting Microsoft’s BlueKeep patch

- Will BlueKeep Become WannaCry 2.0?
  [https://www.bitsight.com/blog/will-bluekeep-become-wannacry-2.0](https://www.bitsight.com/blog/will-bluekeep-become-wannacry-2.0)

- The much-publicized BlueKeep threat has finally emerged – why should you care?
  [https://blog.avast.com/what-is-bluekeep](https://blog.avast.com/what-is-bluekeep)

- Debunking The BlueKeep Exploit Hype – What You Should Know

- Remove syscall hook from BlueKeep payload
  [https://github.com/rapid7/metasploit-framework/pull/12553](https://github.com/rapid7/metasploit-framework/pull/12553)
Questions
Questions

Upcoming Briefs

• Incident Response
• Emotet Update

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.
HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

About Us

Products

Sector & Victim Notifications
Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar
Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

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

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV