



## Remote Desktop Puzzle Reconstrucția Silențioasă a Activității

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                               |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Descriere                     | Un nou vector de atac denumit „ <b>Remote Desktop Puzzle</b> ” permite atacatorilor să extragă informații sensibile din fișierele de cache grafic generate de sesiuni <b>Remote Desktop Protocol</b> (RDP), chiar și în absența jurnalelor tradiționale. Această tehnică vizează sistemele Windows care folosesc optimizările grafice ale <b>RDP</b> , în special <b>bitmap caching</b> , lăsând în urmă „urme vizuale” ale sesiunilor anterioare.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                               |
| Mecanismul tehnic al atacului | <ol style="list-style-type: none"><li>1. Comportamentul <b>RDP</b>: pentru a reduce latența și consumul de bandă, protocolul <b>RDP</b> utilizează un sistem de cache <b>bitmap</b> care salvează local plăci (tiles) grafice, precum ferestre, iconițe și text.</li><li>2. Persistența datelor: chiar după închiderea sesiunii <b>RDP</b> și delogare, fișierele <b>.bmc</b> rămân stocate în:<br/><b>C:\Users\&lt;username&gt;\AppData\Local\Microsoft\Terminal Server Client\Cache\</b></li><li>3. Exploatarea: un atacator care are acces la sistem poate:<ul style="list-style-type: none"><li>• șterge logurile tradiționale (ex: Security, TerminalServices, Event Logs) pentru a-și acoperi urmele;</li><li>• lăsa cache-ul <b>bitmap</b> intact, care nu este monitorizat de majoritatea sistemelor <b>EDR</b>.</li></ul></li><li>4. Instrumente de analiză utilizate:<ul style="list-style-type: none"><li>• <b>BMC-Tools</b>: extrage imaginile <b>bitmap</b> din fișierele <b>.bmc</b>;</li><li>• <b>RdpCacheStitcher</b>: recompilează ecranul pe baza pozițiilor și dimensiunilor fragmentelor extrase;</li><li>• Alte scripturi <b>Python</b> pentru colaj automatizat și <b>OCR</b> pentru extragerea de text.</li></ul></li></ol> |                                                               |
| Vectori de atac               | <ul style="list-style-type: none"><li>• Atac local post-exploatare: atacatorul are deja acces (fizic, RCE, malware).</li><li>• <i>Threat Persistence și Forensics Evasion</i>: eliminarea logurilor dar păstrarea datelor vizuale exploatabile.</li><li>• Reconstrucție post-mortem: chiar și după restaurarea sistemului, imaginile din cache pot fi analizate retrospectiv.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                               |
| Măsurile de detecție          | <ul style="list-style-type: none"><li>• Scanarea manuală - Verificați existența folderelor <b>.bmc</b> în <b>AppData\Local\Microsoft\Terminal Server Client\Cache\</b></li><li>• Monitorizare <b>EDR</b> - Configurați alertare pentru acces/modificare fișiere <b>.bmc, .bin, .dat</b>.</li><li>• Analiza de răspuns la incident - Includeți analiza cache-ului <b>RDP</b> în toate playbook-urile <b>IR</b>, în special dacă logurile lipsesc.</li><li>• Scripturi <b>PowerShell</b> de control - Automate de listare și ștergere cache <b>RDP</b> pe sistemele finale.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                               |
| IOCs                          | Tip                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Indicator                                                     |
|                               | Path fișiere cache RDP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>%LOCALAPPDATA%\Microsoft\Terminal Server Client\Cache\</b> |
|                               | Extensii suspecte                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>.bmc, .bin, .dat</b>                                       |



## Remote Desktop Puzzle Reconstrucția Silențioasă a Activității

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                 |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
|                                            | Tool-uri utilizate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>BMC-Tools</b> , <b>rdpcachestitcher.py</b> ,<br><b>bitmapcache_parser.py</b> |
|                                            | Comenzi PowerShell                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>Get-ChildItem -Path</b><br><b>\$env:LOCALAPPDATA\*\Cache -Recurse</b>        |
|                                            | Pattern de fișiere mari                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | bitmap1.bin > 5MB sau sute de bitmapX.bmc în folder                             |
| <b>Politici GPO/Scripturi de prevenire</b> | <ol style="list-style-type: none"><li>1. GPO – Ștergere automată a cache-ului la logoff:<ul style="list-style-type: none"><li>• Setare script <b>logoff.bat</b>:<br/>„del /f /q \"%LOCALAPPDATA%\Microsoft\Terminal Server Client\Cache\*\" ”</li><li>• PowerShell (versiune enterprise):<br/>„\$CachePath = \"\$env:LOCALAPPDATA\Microsoft\Terminal Server Client\Cache\"<br/>if (Test-Path \$CachePath) {<br/>    Remove-Item \"\$CachePath\*\" -Force<br/>} ”</li></ul></li></ol>                                                                                                                                                                                                                                                                                                                                              |                                                                                 |
| <b>Recomandări de remediere</b>            | <ol style="list-style-type: none"><li>1. Politici automate de curățare - Curățare periodică a conținutului cache RDP (prin GPO, scripturi sau taskuri programate).</li><li>2. Restricții de acces - Drepturi limitate pentru utilizatorii standard asupra folderelor cache RDP.</li><li>3. Dezactivarea bitmap caching (unde nu este necesar):<br/>„[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services]<br/>"BitmapCacheSize"=dword:00000000 ”</li><li>4. Activarea NLA (Network Level Authentication - Previne accesul RDP fără autentificare la nivel de rețea, adăugând un strat suplimentar de securitate.</li><li>5. Actualizare și monitorizare endpoint - Integrare cu EDR care monitorizează fișiere temporare și artefacte neobișnuite (ex: SentinelOne, CrowdStrike, Defender ATP).</li></ol> |                                                                                 |
| <b>Referințe</b>                           | <a href="https://cybersecuritynews.com/remote-desktop-puzzle/">https://cybersecuritynews.com/remote-desktop-puzzle/</a><br><a href="https://csrc.nist.gov/pubs/sp/800/115/final">https://csrc.nist.gov/pubs/sp/800/115/final</a><br><a href="https://learn.microsoft.com/en-us/azure/virtual-desktop/rdp-properties?context=%2Fwindows-server%2Fcontext%2Fwindows-server-remote-desktop-services">https://learn.microsoft.com/en-us/azure/virtual-desktop/rdp-properties?context=%2Fwindows-server%2Fcontext%2Fwindows-server-remote-desktop-services</a>                                                                                                                                                                                                                                                                         |                                                                                 |