AL2025_05 New Process Hollowing Attack Vectors Uncovered in Windows 11 (24H2) (03rd February 2025)

Description

Process Hollowing is a code injection technique commonly employed by malware to evade detection. It involves creating a legitimate process in a suspended state, hollowing out its memory, and replacing it with malicious code. Once resumed, the process appears legitimate while executing harmful actions in disguise. This method has been effective in bypassing traditional security measures. The Windows 11 version 24H2 update, released on October 1, 2024, introduced changes to improve performance and security. However, these updates unintentionally affected traditional Process Hollowing techniques, giving rise to new attack methods.

Attack Details

In Windows 11 version 24H2, the Windows loader's behavior during process initialization was modified to support Hotpatching. A key change involves the loader calling the function ZwQueryVirtualMemory with a parameter that requires memory regions to be flagged as MEM_IMAGE. Traditional Process Hollowing techniques typically use MEM_PRIVATE memory allocations for injected payloads. This mismatch causes the process to terminate with an error code 0xC0000141.

While this change complicates the use of traditional Process Hollowing by attackers, it also affects legitimate tools and research frameworks that rely on this technique for penetration testing or debugging purposes. In response, attackers are adapting by employing alternative methods such as Process Doppelganging, Process Ghosting, and hybrid techniques like Transacted Hollowing. These approaches map payloads as MEM_IMAGE, bypassing the new restrictions while maintaining stealth.

Remediation

To mitigate the risks associated with these evolving attack vectors, consider the following strategies:

1. **Behavioral Monitoring**: Implement advanced monitoring solutions that focus on detecting anomalous behaviors rather than relying solely on signature-based detection.
2. **Memory Analysis**: Regularly perform memory analysis to identify suspicious memory allocations and modifications within processes.

3. **Endpoint Protection**: Ensure that endpoint protection solutions are updated to recognize and respond to these new injection techniques.
4. **System Hardening**: Apply the latest security patches and updates to operating systems and applications to reduce vulnerabilities that could be exploited by these techniques.
5. **Security Training**: Educate security teams about these emerging threats and the importance of monitoring for behavioral indicators of compromise.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

Baran, G. (2025, February 3). New process hollowing attack vectors uncovered in Windows 11 (24H2). Retrieved from *Cyber Security News*. https://cybersecuritynews.com/process-hollowing-attack-windows-11/

Process injection: Process hollowing, sub-technique T1055.012 - Enterprise | MITRE ATT&CK®. . https://attack.mitre.org/techniques/T1055/012/