InfoSec Handlers Diary Blog - Preempting a Major Issue Due to the LNK Vulnerability

We decided to raise the Infocon level to Yellow to increase awareness of the recent LNK vulnerability and to help preempt a major issue resulting from its exploitation. Although we have not observed the vulnerability exploited beyond the original targeted attacks, we believe wide-scale exploitation is only a matter of time. The proof-of-concept exploit is publicly available, and the issue is not easy to fix until Microsoft issues a patch. Furthermore, anti-virus tools' ability to detect generic versions of the exploit have not been very effective so far.

Although the original attack used the LNK vulnerability to infect systems from a USB key, the exploit can also launch malicious programs over SMB file shares. In one scenario, attackers that have access to some systems in the enterprise can use the vulnerability to infect other internal systems.

We discussed the LNK vulnerability in a diary a few days ago. That note pointed to Microsoft's advisory that described the bug "Windows Shell Could Allow Remote Code Execution," which affects most versions of Windows operating systems. Microsoft's workarounds for the issue include:

- Disable the displaying of icons for shortcuts. This involves deleting a value from the registry, and is not the easiest thing to do in some enterprise settings. Group Policy-friendly options include the use of Registry Client-Side Extensions, the regini.exe utility and the creation of a custom .adm file: see Distributing Registry Changes for details.
- Disable the WebClient service. This will break WebDAV and any services that depend on it.

Another approach to mitigate the possible LNK attack involves the use of Didier Stevens' tool Ariad. Note that the tool is beta-software operating in the OS kernel, so it's probably not a good match for enterprise-wide roll-out.

Additional recommendations for making the environment resilient to an attack that exploits the LNK vulnerability include:

- Disable auto-run of USB key contents. This would address one of the exploit vectors. For instructions, see Microsoft KB967715.
- Lock down SMB shares in the enterprise, limiting who has the ability to write to the shares.

Sadly, enterprises that are likely to ever disable auto-run and lock down SMB file shares, probably have done this already back when the Conficker

worm began spreading. Another challenge is that Windows 2000 and Windows XP Service Pack 2 are vulnerable, yet Microsoft no longer provides security patches for these OS. As the result, we believe most environments will be exposed until Microsoft releases a patch. We're raising the Infocon level in the hope that increased vigilance will increase enterprises' ability to detect and respond the attacks that may use the LNK vulnerability.

Update: Several readers recommended focusing on preventing unauthorized code from running by using approaches such as application whitelisting. For instance, Richard and Erno mentioned AppLocker, which is an enterprise software control feature built into Windows 7. Erno wrote, "My solution is standard user accounts and Software Restriction Policy or AppLocker in Group Policy. You can block execution of any files on removable drives or network drives, or actually pretty much anywhere except system folders. In my networks I only allow execution from Windows and Program Files. Remember to apply the software restriction policy for all executable files, including libraries (dlls)." By the way, this is the kind of approach Jason Fossen and I explore in the new course we are about to debut, called Combating Malware in the Enterprise.

Do you have recommendations for addressing the LNK issue? Let us know.

-- Lenny

Lenny Zeltser - Security Consulting
Lenny teaches how to analyze and combat at SANS Institute. You can find him on Twitter.