MSUpdater Trojan And Link To Targeted Attacks | Zscaler

By ThreatLabz

Published: 2012-01-31 · Archived: 2026-04-05 17:11:31 UTC

This blog post is based on a joint report by Zscaler and Seculert. Researchers from both companies separately identified attacks which used a remote access tool (RAT) malware that apparently targeted defense-related organizations. With joined forces, we analyzed the incidents that we observed and those published in the open-source to identify attack patterns and incidents from early 2009 to present.

Figure 1: Screenshot of Report Heading

The threat arrives in phishing emails with a PDF attachment, possibly related to conferences for the particular targeted industry. The PDF exploits a vulnerability within Adobe (for example, a 0-day exploit was used against CVE-2010-2883) which then drops a series of files to begin communicating with the command and control (C&C).

Figure 2: Screenshot of Example Conference PDF "Lure"

The malware dropped and launched from the PDF exploit has been seen to be virtual machine (VM) aware in order to prevent analysis within a sandbox. The Trojan functionality is decrypted at run-time, and includes expected functionality, such as, downloading, uploading, and executing files driven by commands from the C&C. Communication with the C&C is over HTTP but is encoded to evade detection. The Trojan file name (e.g.,

"msupdate.exe") and the HTTP paths used in the C&C (e.g., "/microsoftupdate/getupdate/default.aspx") are used to stay under the radar by appearing to be related to Microsoft Windows Update - hence the name given to this Trojan.

Correlating this information with open-source intelligence (OSINT), we were able to find other reports of this Trojan within past targeted incidents, as well as a link to other incidents and compromise indicators. Further details of this information can be read within our joint report. The mission of this report is to inform organizations and security executives about these threats, and assist them in detection and mitigation.

Explore more Zscaler blogs
