Endpoint Protection

symantec.com/connect/blogs/backdoorbarkiofork-targets-aerospace-and-defense-industry

Back to Library

Backdoor.Barkiofork Targets Aerospace and Defense Industry

1 Recommend

Jan 30, 2013 06:01 PM

Migration User

Contributor: Joseph Bingham

A few weeks ago, we observed a spear phishing campaign targeting groups in the aerospace and defense industry. We identified at least 12 different organizations targeted in this attack. These organizations include aviation, air traffic control, and government and defense contractors.

Figure 1. *Spear phishing email targeting aerospace and defense industry*

In choosing their targets, the attackers identified individuals in important roles, including directors and vice presidents. The content of all the emails were identical. The attackers used a report published in 2012 regarding the outlook of the aerospace and defense industries as the lure. The intention of the attackers was to make it seem as though this email originally came from the company that authored the report. The emails were also crafted to look as though they were being forwarded by internal employees or by individuals from within the industries identified.

When the malicious PDF attached to the email is opened, it attempts to exploit the Adobe Flash Player CVE-2011-0611 'SWF' File Remote Memory Corruption Vulnerability (CVE-2011-0611). If successful, it drops malicious files as well as a clean PDF file to keep the ruse going.

Figure 2. *Clean PDF file displayed to the user*

The clean PDF file that is dropped is the industry report identified as the lure, however, it curiously has been modified by the attackers to remove some branding elements.

In addition to the clean PDF file, the threat drops a malicious version of the svchost.exe file. This file then drops a malicious version of ntshrui.dll into the Windows directory. The threat leverages a technique known as DLL search order hijacking (the ntshrui.dll file is not protected by KnownDLLs). When the svchost.exe file calls the explorer.exe file, it will load the malicious ntshrui.dll file in the Windows folder instead of the legitimate ntshrui.dll file in the Windows system directory. Symantec detects both the svchost.exe and ntshrui.dll files as Backdoor.Barkiofork.

This version of Backdoor.Barikiofork has the following capabilities:

- Enumerates disk drives
- Contacts the command-and-control (C&C) server at osamu.update.ikwb.com
- Steals system information
- Downloads and executes further updates

This spear phishing campaign continues to show the sophistication and preparation of attackers, especially gathering intelligence on what social engineering will best entice targets.

Organizations should ensure proper email security is in place and also make patch management a priority, as the vulnerability exploited here was patched in 2011.

Statistics

0 Favorited

0 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.