Newly discovered Chinese hacking group hacked 100+ websites to use as “watering holes”

By Sean Gallagher

Published: 2015-08-05 · Archived: 2026-04-05 17:13:47 UTC

LAS VEGAS—Today at the Black Hat information security conference, Dell SecureWorks researchers unveiled a report on a newly detected hacking group that has targeted companies around the world while stealing massive amounts of industrial data. The majority of the targets of the hacking group were in the automotive, electronic, aerospace, energy, and pharmaceutical industries. The group, believed to be based in China, has also targeted defense contractors, colleges and universities, law firms, and political organizations—including organizations related to Chinese minority ethnic groups.

Designated as Threat Group 3390 and nicknamed “Emissary Panda” by researchers, the hacking group has compromised victims’ networks largely through “watering hole” attacks launched from over 100 compromised legitimate websites, sites picked because they were known to be frequented by those targeted in the attack.

At least 50 organizations in those industries in the US and the United Kingdom had data stolen by members of Emissary Panda. Sites targeted included the website of the Embassy of the Russian Federation in the US (as well as those of other embassies and non-governmental organizations); government agency websites around the world; manufacturing companies, many of whom were suppliers to defense contractors; and the Spanish defense manufacturer Amper. A cultural site for the Chinese Uyghur ethnic group was also used, apparently to target members of the Muslim minority for surveillance.

No zero-day vulnerabilities were used to breach targeted networks, instead “the group relied on old vulnerabilities such as CVE-2011-3544”—a near-year-old Java security hole—“and CVE-2010-0738 to compromise their targets,” Dell SecureWorks’ researchers reported. The group used a number of tools common to other Chinese hacking groups, but they had a few unique tools of their own with interfaces developed for Standard (Simplified) Chinese. One of these is the PlugX remote access tool, “a notorious piece of malware linked to a number of attacks and to another Threat Group, which researchers believe is also likely based out of China,” according to Dell SecureWorks researchers. It also appears the group used China’s Baidu search engine to perform reconnaissance on targets.
