MITRE-ID: G0031

Name: Dust Storm

Country: China

Description:

Dust Storm is a threat group that has targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries.

TTPs:

1. Very little public information was available throughout 2010 on this threat, despite the group’s primary backdoor gaining some level of prominence in targeted Asian attacks. This may be explained by the group’s early reliance on Dynamic DNS domains for their command and control (C2) infrastructure, as well as their use of public RATs like Poison Ivy and Gh0st RAT for second-stage implants.
2. It wasn’t until June 2011 that Operation Dust Storm started to garner some notoriety from a series of attacks which leveraged an unpatched Internet Explorer 8 vulnerability, CVE-2011-1255, to gain a foothold into victim networks. In these attacks, a link to the exploit was sent via a spear phishing email from a purported Chinese student seeking advice or asking the target a question following a presentation.
3. As to other documented cases, the attacker started interacting with the infected machine within minutes of compromise to begin manual network and host enumeration.
4. In October 2011, the group attempted to take advantage of the ongoing Libyan crisis at the time and phish the news cycle regarding Muammar Gaddafi’s death on October 20, 2011. It appears that in addition to some US defense targets, this campaign was also directed at a Uyghur mailing list. This time, the group used a specially crafted malicious Windows Help (.hlp) file, which exploited CVE-2010-1885.
5. Dust Storm has encoded payloads with a single-byte XOR, both skipping the key itself and zeroing to avoid exposing the key.
6. Dust Storm has used Android backdoors capable of enumerating specific files on the infected devices.
7. Dust Storm has used Android backdoors capable of exfiltrating specific files directly from the infected devices.