Dust Storm - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:19:19 UTC

APT group: Dust Storm

Names	Dust Storm *(Cylance)* G0031 *(MITRE)*
Country	China
Sponsor	Seems state-sponsored
Motivation	Information theft and espionage
First seen	2010
Description	(Cylance) 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. 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. As to other documented cases, the attacker started interacting with the infected machine within minutes of compromise to begin manual network and host enumeration. 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.
Observed	Sectors: Energy, Oil and gas and Uyghurs. Countries: Japan, South Korea, USA and Europe and Southeast Asia.
Tools used	Gh0st RAT, Misdat, MiS-Type, Poison Ivy, S-Type.

Information	<https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf> <https://www.symantec.com/connect/blogs/inside-back-door-attack>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0031/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
