砂嵐大作戦

# OPERATION DUST STORM ATTACK TIMELINE

## 2010

Early operations are extremely blunt, relatively unsophisticated, and readily picked up by the security industry.

## 2011

Attacks leverage an unpatched Internet Explorer 8 vulnerability to gain a foothold into victim networks and start to garner some notoriety.

## October 2011

Attack group attempts to take advantage of the ongoing Libyan crisis by phishing the news cycle regarding Muammar Gaddafi's death, targeting US defense targets.

## July to August 2011

Attack group attempts to gather user credentials for Yahoo, Windows Live, and other accounts through several different phishing domains.

## June 2012

Attack campaign leverages previously used flash exploit and Internet Explorer zero-day.

## March to August 2013

Attack activity greatly subsides, although several new domains that will be used later are registered.

## 2015

A number of second-stage backdoors with hardcoded proxy addresses and credentials compromise a number of Japanese companies involved in power generation, oil and natural gas, construction, finance, and transportation.

## February 2014

Watering hole attack on a popular software reseller delivers an Internet Explorer zero-day to a number of unsuspecting targets. The group begins locating and securing alternative means of persistence on victim systems.

## February 2015

A second-stage implant delivered by a variant of the S-Type backdoor shortly following its initial reconnaissance compromises the investment arm of a major Japanese Automaker just two weeks before 11 auto worker unions demand a monthly raise of 6,000 yen.

## July & October 2015

Two new waves of attacks are launched, targeting multiple Japanese companies including a Japanese subsidiary of a South Korean electric utility and a major Japanese oil and gas company. The most likely goals are reconnaissance and long-term espionage.

## May 2015

Attack group adopts and customizes several Android backdoors to suit their purposes and uses a massive infrastructure compared to previous attacks. Initial backdoors are relatively simple, but continually forward all SMS messages and call information back to their C2 servers. All identified victims reside in Japan or South Korea.

## 2016

SPEAR believes that attacks of this nature into companies involved in Japanese critical infrastructure and resources are ongoing and likely to continue to escalate in the future.

CYLANCE