DUST STORM

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON DUST STORM ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Dust Storm is a threat group based out of China whose main motivations include Information theft and espionage .

II. TARGETS

Attacks of this threat group ranges around henergy , oil and gas also the Uyghurs in countries like Japan , South Korea , US and parts of Europe & Southeast Asia .

III. METHODS USED

This group uses Internet Explorer 8 vulnerability , CVE-2011-1255 to gain a foothold into victim network .
This group also has been using spear phishing as one of it's techniques against the vtarget .
This group has also used specially crafted malicious windows help (.hlp) file , which exploited CVE-2010-1885.
This group has also been using public RATs like Poson Ivy and Gh0st RAT for secons stage implants .

IV. CAMPAIGNS

This group has been involved in operation Dust Storm.
This group has also been involved in taking advantage of the ongoing Libyan crisis as the time and phish the news cycle regarding Gaddafi's death .

ATTRIBUTION

As per Cylance , this APT group has been attributed to China .

[cited from ThaiCERT]

V. IOCS

Gh0st RAT IOCs

Mozilla.exe
EE04B324F7E25B59D3412232A79D1878632D6817C3BB49500B214BF19AFA4E2C

Updateproxy.dll
0BA49FEB7784E6D33D821B36C5C669D09E58B6795ACA3EEBBF104B763B3B3C20

Telnet.dll
33B7407E534B46BF8EC06D9F45ECD2D3C7D954340669E94CD7CEDCBAE5BAD2DD

Socks.dll
6160AF383794212B6AD8AB9D6D104BBE7AEFB22410F3AB8EA238F98DABFC48B7

Shell.dll
C63B01C40038CA076072A35913F56D82E32FCEE3567650F3392B5C5DA0004548

Session.dll
D51EC4ACEAFA971E7ABD0CF4D27539A4212A448268EF1DB285CD9CE9024D6EB3

Screen.dll
BD8086DE44E16EFDD380E23E49C4058D956538B01E1AE999B679B6B76B643C7D

Port.dll
B44A9545B697B4D46D5B96862A6F19EA72F89FED279F56309B2F245AC8380BE0

File.dll
F4DF97108F18654089CFB863F2A45AA41D17A3CE8A44CCCC474F281A20123436

ConEmu.exe
D31D38403E039F5938AE8A5297F35EB5343BB9362D08499B1E07FAD3936CE6F7

Noodles.exe
A591D4D5B8D23FF12E44A301CE5D4D9BF966EBA0FC0068085B4B4EC3CE352963

Coal.exe (Malicious executable)
EEBFF21DEF49AF4E85C26523AF2AD659125A07A09DB50AC06BD3746483C89F9D

Abg.exe (Malicious executable)
97B9D7E16CD6B78A090E9FA7863BD9A57EA5BBE6AE443FA788603EEE5DA0BFC3

23d.exe (Malicious executable)
B6C21C26AEF75AD709F6C9CFA84BFA15B7EE709588382CE4BC3544A04BCEB661

89d.exe (Malicious executable)
DB9B9FA9EFA53662EC27F4B74B79E745F54B6C30C547A4E5BD2754E9F635F6DB

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Dust%20Storm

https://attack.mitre.org/groups/G0031/