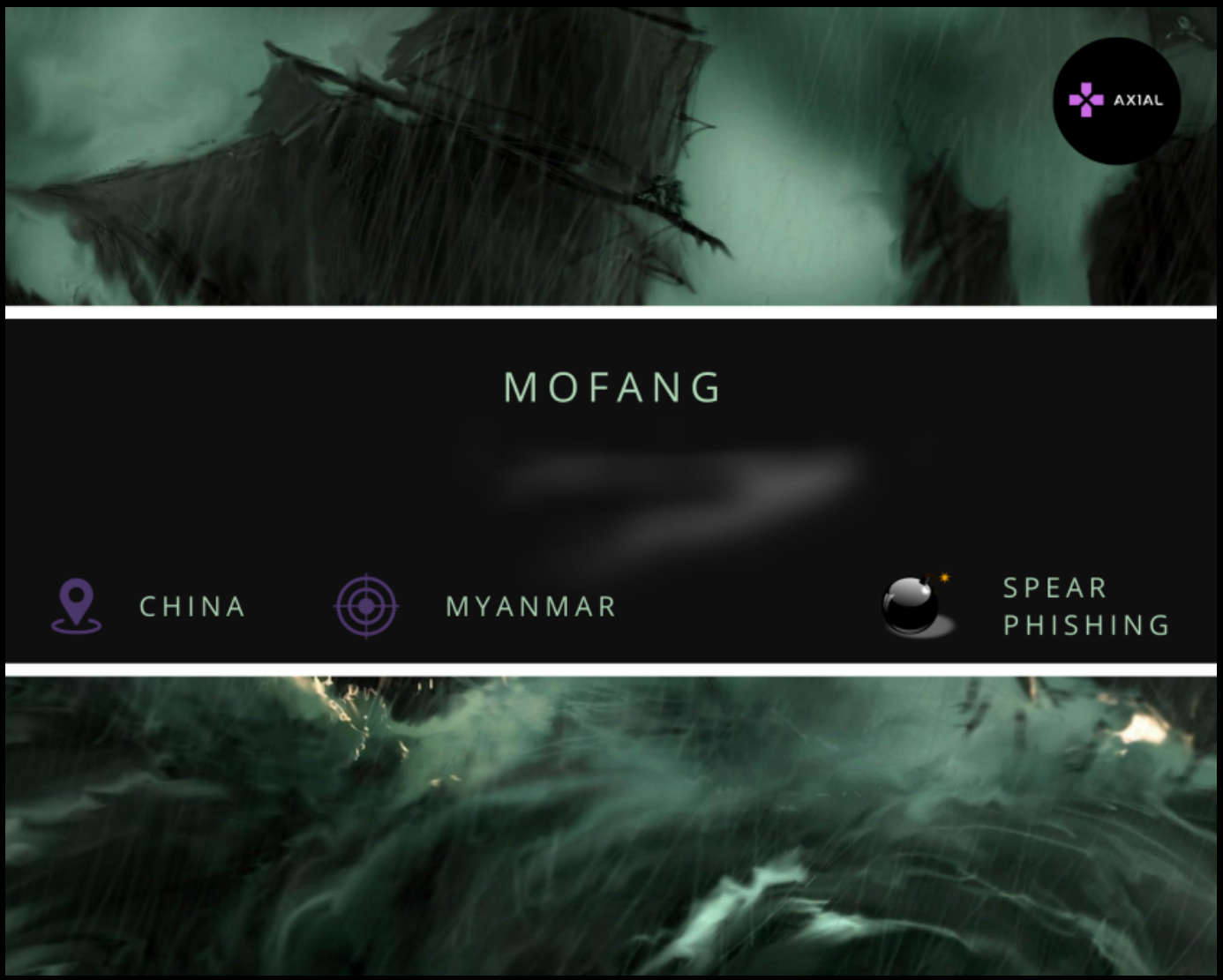
MOFANG



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON MOFANG: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Mofang is a cyber-espionage group based out of China that has targeted various countries and is probably government affiliated , it also goes by various names like Whitefly , ATK 83 , SectorM04 which mostly focuses on critical information theft.

II. TARGETS

Mofang has been targeting those investments or technological advances that somehow is related to China , also they have been focusing on Myanmar and it's critical infrastructure and political artifacts , they also have been targeting various critical artifacts onto vmultiple countries.

III. METHODS USED

MOFANG uses privilege elevation exploits builT into their own malware .
MOFANG uses distinct tools ShimRat and ShimRatReporter .
MOFANG group also uses social engineering as one of their attack vectors.
MOFANG also uses Shims in windows to build up persistence , shims are hot patching process on the fly , to ensure backward compatibility of software on the Microsoft Windows
MOFANG has also been using open-source hacking tools and living off land tactics such as malicious Powershell Scripts.

IV. CAMPAIGNS

- Mofang has been involved in attack on Singapore's largest public health organization also known as SingHealth which resulted in 1.5 million patient records being stolen .
- Mofang has also hit a Canadian Organization in January 2013, later they continued their attacks onto unknown organizations.
- Mofang has also launched multiple attacks on Myanmar government entity , and South Korean Companies also the US based companies .
- Mofang has also continued it's attacks onto Myanmar based government entities onto 2015 and various organizations.

ATTRIBUTION

Mofang almost operated out of China and is probably government affiliated , it's targets are based on involvements or investments that potentially posses a threat to China , some reports also have validated that it's activities have links to a bid on an oil and gas pipeline project in Myanmar

[cited from Fox-IT reports]

AX1AL

V. IOCS

MD5 Hashes

f4b247a44be362898c4e587545c7653f
e79b2d2934e5525e7a40d74875f9d761
6b126cd9a5f2af30bb-048caef92ceb51
4e493a649e2b87e-f1a341809dab34a38
d8b95e942993b979fb82c22e-a5b5ca18
c27fb6999a0243f-041c5e387280f9442
b4554c52f708154e529f62ba8e0de084
8c85d527340a17d267379bcd9e5e5bf
3eb9d4c448cd5ec8cb49fa1e3b42b75
663e54e686842eb8f8bae2472cf01ba1

C2's

http://video.today-nytimes.com/en-us/b/index.php
http://www.goodlook.sg/po/index.php
https://api.officeonlinetool.comindex.php
https://ie.update-windows-microsoft.com/update/index.php
http://travel.tripmans.com/links/images/links.php
http://dns.undpus.com/index.php
https://secure2.sophosrv.com/en-us/support/ms-cache_check.php
https://ie.update-windows-microsoft.com/my/js/index.php
http://www.tinroofpopcorn.com/admin/fckeditor/_samples/_plugins/samples.php

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Whitefly%2C%20Mofang
https://attack.mitre.org/groups/G0005/

https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

https://news.softpedia.com/news/chinese-apt-targets-victims-with-social-engineering-and-shimrat-malware-505255.shtml

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore