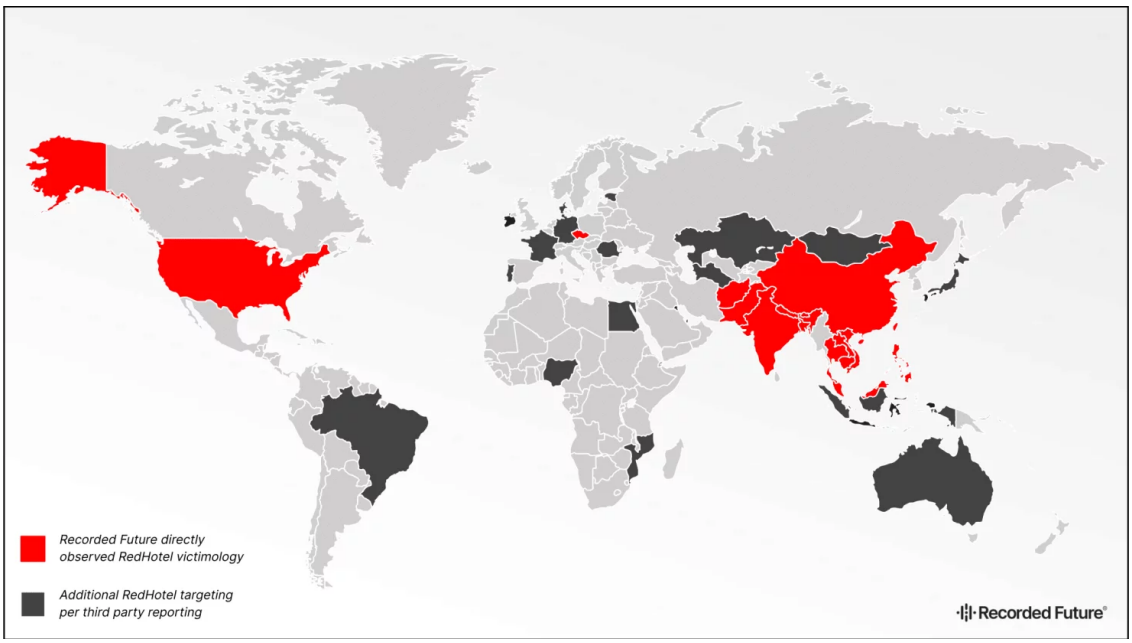
RedHotel: Threat group targets 17 countries in 3 years, including Nigeria.

A recent threat analysis by Recorded Future indicated that a threat group named RedHotel had compromised many government organisations worldwide, including Nigeria.

RedHotel is an Advanced Persistent Threat (APT) likely sponsored by the Chinese government that targets sectors in telecommunications, academia, government, research, religious groups, media, cryptocurrency and financial organisations for espionage purposes.

The Targets



The Victim map ¦ Credit: Recorded Future

According to the Malicious Traffic Analysis data, victims included the United States, Palestine, Afghanistan, Nepal, Malaysia, Taiwan, Thailand, the Philippines and India amongst others. Third party reporting indicated that Nigeria, Egypt, Ireland, Brazil, and Australia were part of the victim list.

The majority of victims were government bodies while others were observed to be industrial and economically important ones. These included the Technology Research Institute in Taiwan, Hong Kong pro-democracy groups, and online gambling companies.

It is to be noted that this is not the first time RedHotel has made the news. On January 17, 2022, Trend Micro released a report on the group which it dubbed 'Earth Lusca'. It noted that the primary motivation of the group was cyberespionage and it used three primary attack vectors: Spear phishing, watering holes and vulnerability exploitation.

On December 9, 2021, Crowdstrike's OverWatch reported in a blogpost that it had intercepted an attack by the threat group trying to exploit the Log4j vulnerability on a vulnerable system in an academic institution. Overwatch also indicated that the group used Cobalt Strike, a legitimate commercial penetration testing tool, in its attack.

Threat Profile

Here's some basic information about the group and its attributes:

Threat Group: RedHotel

Origin: China, 2019

Other Names: Earth Lusca, Aquatic Panda, TAG-22, BRONZE UNIVERSITY

Targets: Foreign intelligence, industrial and economic espionage, tech, and Covid-19 research

Target Region(s): Northern America, South and East Asia, Western Europe. Thirdparty reports indicate a possibly worldwide scope.

Tools observed: ShadowPad, Winnti, Cobalt Strike, PlugX, Spyder

Attack Vectors: Spear phishing, Watering whole attacks, vulnerability exploitation

Mitigations

Individuals and organisations can protect themselves by doing the following:

1. Avoid clicking suspicious email/website links
2. Update all software and public facing infrastructure
3. Use an Antivirus
4. Organisations can implement network segmentation

Carrying out the steps above can reduce the impact of an attack, or even possibly stop one altogether.

By: Daniel Iwugo

Tags: ADVISORY APT CYBERSECURITY ESPIONAGE

RECENT POSTS

The CYSED Dictionary: Email

What is Dark AI?

PDF files more dangerous than Executables – Report reveals

ALL CATEGORIES

Awareness

Bussiness

Child Online Safety

Cybercrime

Cyberdiplomacy