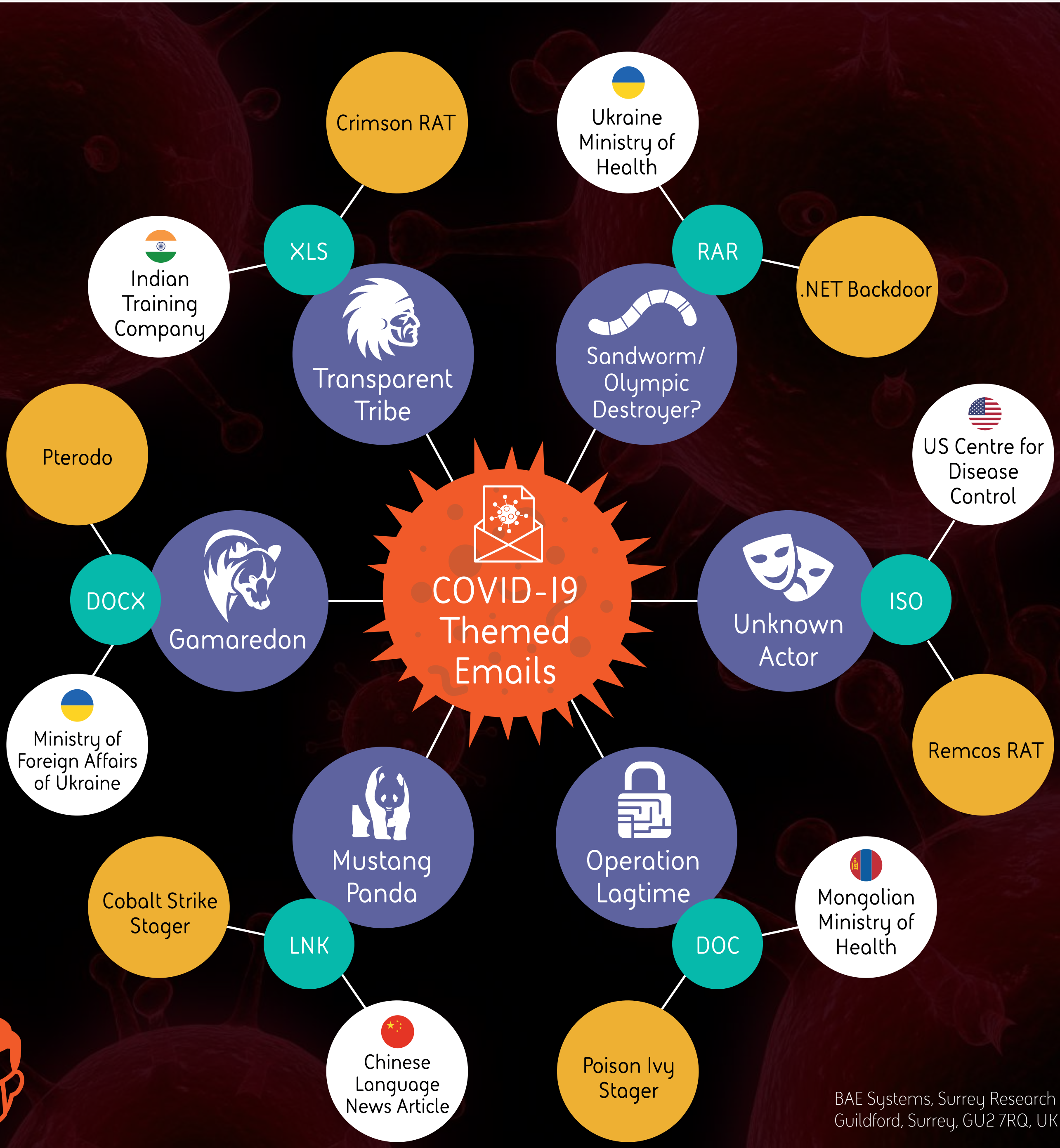
COVID-19 campaigns

Moving into March 2020, countries worldwide are still struggling to manage the spread of the viral disease now known as COVID-19. In cyberspace, threat actors are using the topic of COVID-19 to their advantage with numerous examples of malicious activity using COVID-19 as lure documents in phishing campaigns.

Key/
Phishing Stages

Threat Actor ▶ Delivery File Type ▶ Spoofed Organisation ▶ Payload



COVID-19 Themed Emails

Transparent Tribe
XLS
Indian Training Company
Crimson RAT

Sandworm/ Olympic Destroyer?
RAR
Ukraine Ministry of Health
.NET Backdoor

Unknown Actor
ISO
US Centre for Disease Control
Remcos RAT

Operation Lagtime
DOC
Mongolian Ministry of Health
Poison Ivy Stager

Mustang Panda
LNK
Chinese Language News Article
Cobalt Strike Stager

Gamaredon
DOCX
Ministry of Foreign Affairs of Ukraine
Pterodo

Mitigations

Remind individuals to refrain from opening emails and attachments from untrusted or unfamiliar sources.

If possible, block or monitor file types that are not normally needed for business operations (e.g. ISO files) or should not be delivered as email attachments (e.g. SCR files).

BAE Systems, Surrey Research Park,
Guildford, Surrey, GU2 7RQ, UK

✉ learn@baesystems.com

baesystems.com/threatintel

twitter.com/baesystems_ai

BAE SYSTEMS