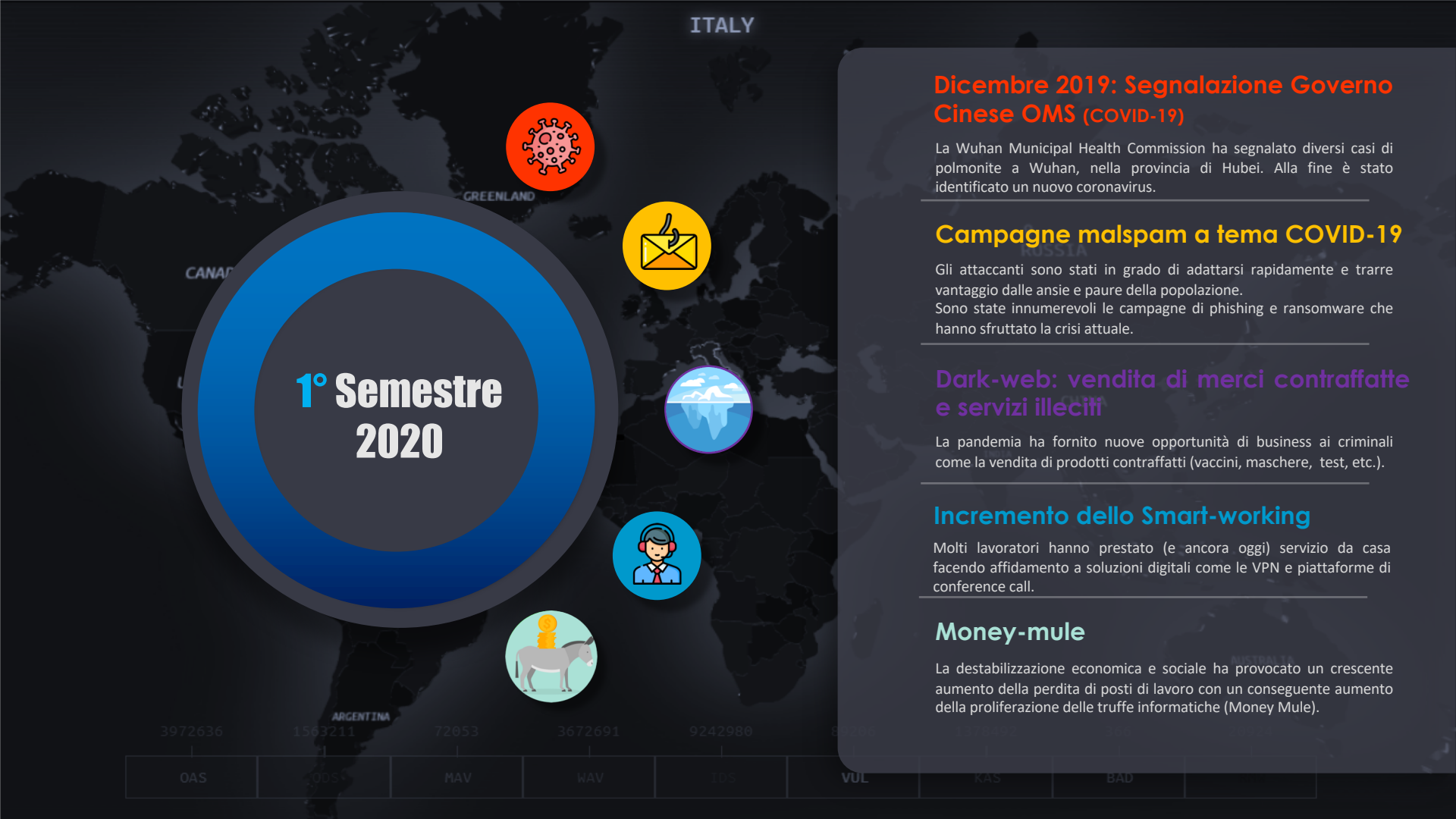

Dicembre 2019: Segnalazione Governo Cinese OMS (COVID-19)

La Wuhan Municipal Health Commission ha segnalato diversi casi di polmonite a Wuhan, nella provincia di Hubei. Alla fine è stato identificato un nuovo coronavirus.

Campagne malspam a tema COVID-19

Gli attaccanti sono stati in grado di adattarsi rapidamente e trarre vantaggio dalle ansie e paure della popolazione.
Sono state innumerevoli le campagne di phishing e ransomware che hanno sfruttato la crisi attuale.

Dark-web: vendita di merci contraffatte e servizi illeciti

La pandemia ha fornito nuove opportunità di business ai criminali come la vendita di prodotti contraffatti (vaccini, maschere, test, etc.).

Incremento dello Smart-working

Molti lavoratori hanno prestato (e ancora oggi) servizio da casa facendo affidamento a soluzioni digitali come le VPN e piattaforme di conference call.

Money-mule

La destabilizzazione economica e sociale ha provocato un crescente aumento della perdita di posti di lavoro con un conseguente aumento della proliferazione delle truffe informatiche (Money Mule).

Malspam: Ritorno in scena di Emotet e Qbot

Molte istituzioni finanziarie hanno segnalato un incremento delle campagne di malspam finalizzate a diffondere i già noti malware Emotet e Qbot.

Campagne Ransom DDoS

Migliaia di organizzazioni in tutto il mondo appartenenti a diversi settori industriali, tra i quali anche il settore finanziario, sono state soggette ad attacchi DDoS accompagnati da note estorsive.

Attacchi ATM

Nella seconda metà del 2020 si è registrato un incremento degli attacchi sferrati ai danni di bancomat e dispositivi ATM mediante tecniche di *ATM Jackpotting*.

Ransomware: chiusura del businessdi Maze

Nel frattempo, la distribuzione di alcune famiglie di malware sembrano perdere di intensità. Questo potrebbe essere il caso del ransomware Maze. In effetti, mentre la notizia del ritiro di Maze fa il giro del mondo, diversi suoi affiliati hanno iniziato a passare a nuove operazioni ransomware (Egregor).

Previsioni 2021

Scam

La depressione economica, causata dalla pandemia, probabilmente porterà un incremento di persone che si avvicina al cyber crime.

RDDoS

Nel 2021 potremmo assistere a nuove ondate di attacchi DDoS di portata e sofisticazione maggiore.

Ransomware

I gruppi ransomware sfrutteranno 0-day exploit, così come n-days exploit (Zerologon), nei prossimi attacchi.