La Cybercriminalite a l'ere du COVID_19:Outils des cybercriminels et methodes de protection

GUY NGONGANG
TWITTER:@MALWARE28

Definitions

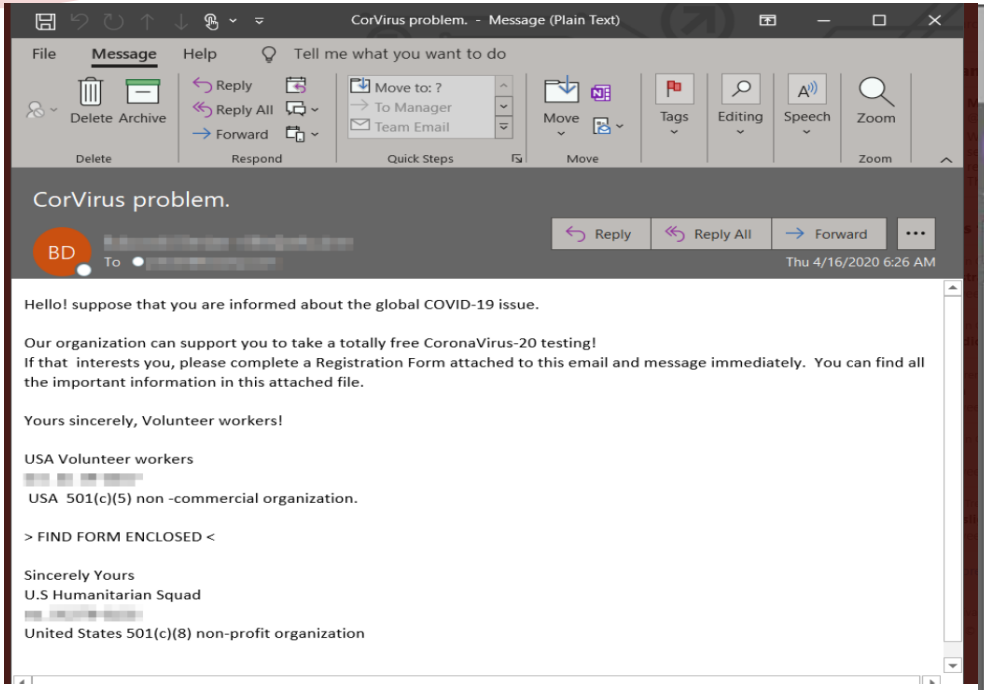
- Malware- Virus, Trojan, Worm
- Cybercriminalite est l‘ensemble des mauvaises pratiques faites par le biais d‘un appareil connecte a internet
- domaine(exemple yahoo.fr, paypal.com)
- Hash est une signature digitale ,identifiant une unique entite
- APT, advanced persistent threat

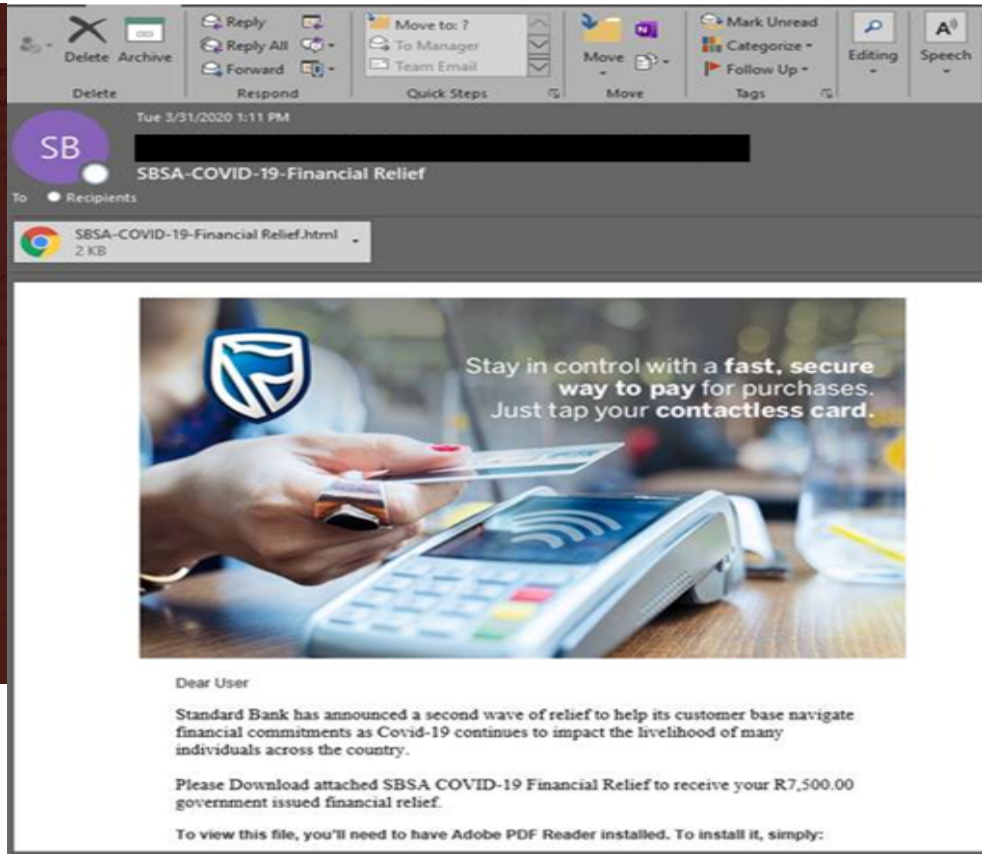
CORONA VIRUS, COVID-19?

- La COVID-19 est la maladie infectieuse causée par le dernier coronavirus qui a été découvert a Wuhan, Chine
- Les symptômes les plus fréquents de la COVID-19 sont la fièvre, la toux sèche et la fatigue.
- La maladie se transmet principalement d'une personne à l'autre par le biais de gouttelettes respiratoires expulsées par le nez ou par la bouche lorsqu'une personne malade tousse, éternue ou parle.
- Il est important de se laver systematiquement les mains et de toujours respecter les règles d'hygiène respiratoire

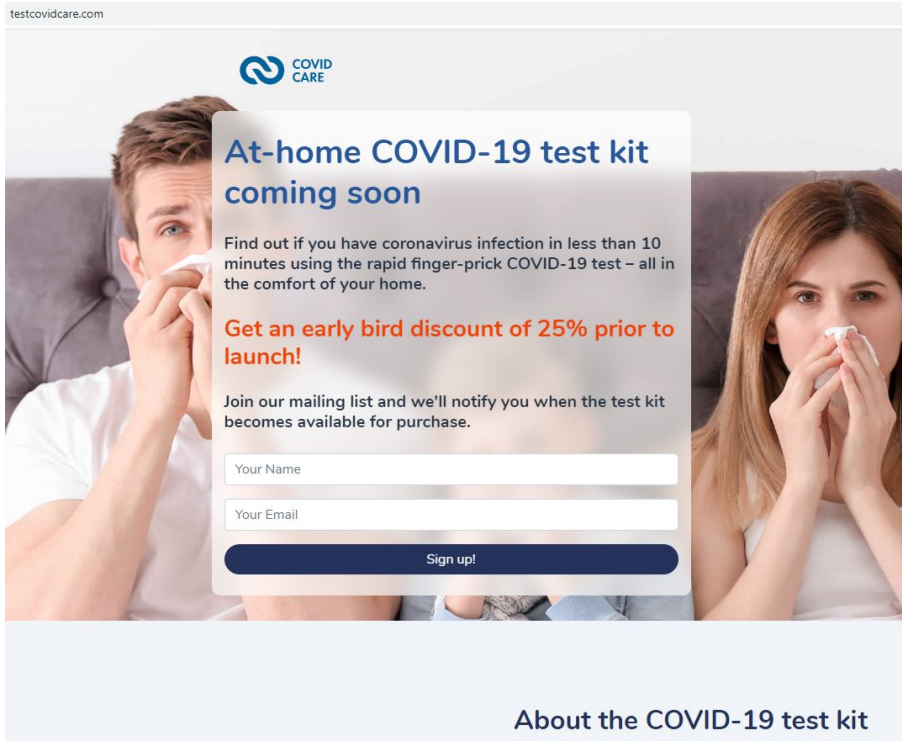
- Pendant cette pandemie, tout le monde travaillait de la maison
- Teletravail a augmente le flux de connection internet
- Les applications se sont vues telechargees en masse (Zoom)

COVID_19 emails scammes(Phishing)





Faux domaines



Due to the recent outbreak for the Coronavirus (COVID-19) the World Health Organization is giving away vaccine kits. Just pay $4.95 for shipping.

You just need to add water, and the drugs and vaccines are ready to be administered. There are two parts to the kit: one holds pellets containing the chemical machinery that synthesises the end product, and the other holds pellets containing instructions that tell the drug which compound to create. Mix two parts together in a chosen combination, add water, and the treatment is ready.

ORDER NOW

- APT34, APT39 : IRAN
- APT41, APT40, APT17: CHINE
- APT37, APT38: COREE DU NORD
- APT29, APT28: GOUVERNEMENT RUSSE
- APT32: VIETNAM

Ransomware, Virus informatiques

- Emotet (dropper)
- Ryuk
- Sodinokibi, publie les informations en cas de non paiement
- Nefilim(unsecured RDP)
- Trickbot (SMB, Ryuk)
- dridex(DopplePaymer)
- Qakbot(Prolock)

VICTIMES

Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

One of the Czech Republic's biggest COVID-19 testing laboratories hit by mysterious cyberattack.

Texas Courts System Hit by Ransomware Attack

11 Ransomware Hit ATM Giant Diebold Nixdorf

MAY 20

Diebold Nixdorf, a major provider of automatic teller machines (ATMs) and payment

Ruhr University Bochum shuts down servers after ransomware attack

Hardware Write Blocker
-Hard disk image
-RAM image

Indicators of compromise

CONCLUSIONS

- Les societes et les hopitaux doivent avoir une processus de reponse aux incidents
- Eduquer les utilisateurs face aux dangers lies a internet
- Mettre a jour les systemes d'exploitations et les applications
- Implementer DKIM pour authentiquer les emails
- Faire des backups
- Bloques les IOCs sur les firewall,proxy, IPS,…
- Scanner les machines pour decouvrir celles infectees et les deconnecter du reseau
- Implementer MFA(Multi-factor Authentication)

REFERENCES

- Organisation mondiale de la sante www.who.int/fr
- Sophos https://news.sophos.com/en-us/2020/04/14/covidmalware/