COVID19 Cybercrime Theme Intrusion using the DIAMOND MODEL

GUY NGONGANG

@malware28

What is COVID19?

- Coronavirus disease (COVID-19) is an infectious disease caused by a newly discovered coronavirus
- The COVID-19 virus spreads primarily through droplets of saliva or discharge from the nose when an infected person coughs or sneezes
- Protect yourself and others from infection by washing your hands or using an alcohol based rub frequently and not touching your face

COVID19 cybercrime Theme

- Fake websites selling COVID19 Vaccines,$4.95

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.

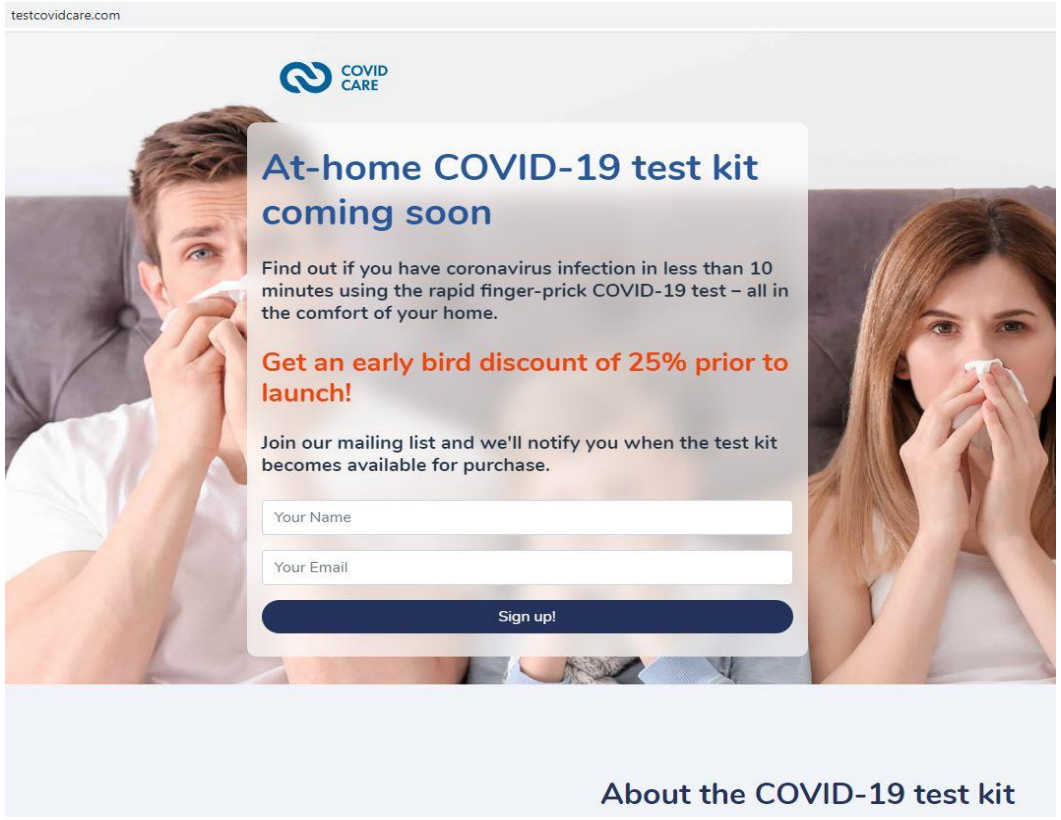
You just need to add water, and the drugs and vaccines are ready to be administered. There are two parts to the kit: one holds pellets containing the chemical machinery that synthesises the end product, and the other holds pellets containing instructions that tell the drug which compound to create. Mix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

ORDER NOW

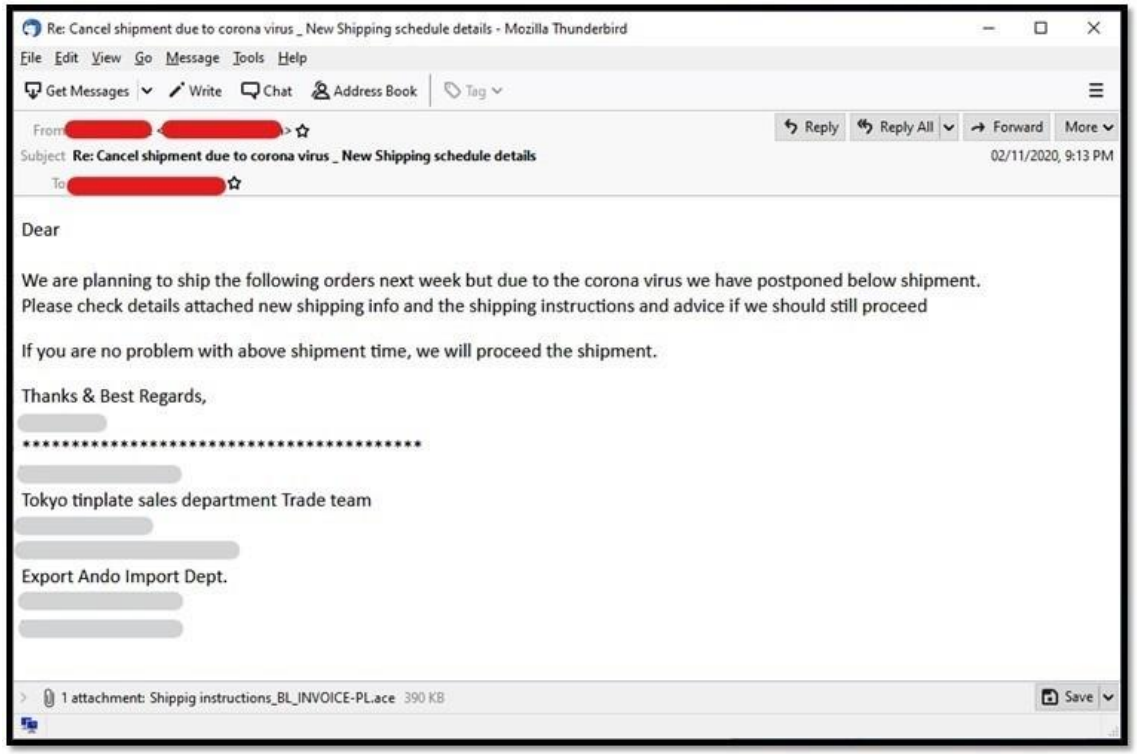
JUST PAY $4.95 FOR SHIPPING

More than 60 fake domains registered like this one below,still up at this date 29.03.2020,21:08 CET time

- https://testcovidcare.com/



Phishing emails targeting English and German speakers,delivering ransomware



In this e-mail, the cybercrook threats infecting all family members if the ransom is unpaid (Extorsion)

From: [redacted]@outlook.com
Subject: c[redacted]
Date: March 19, 2020 at 9:05:05 AM PDT
To: c[redacted]

I know every durty little secret about your life. To prove my poiητ, tell me, does "[redacted]" ring αny bell to you? It was oηe of your ραsswords.

Whaτ do I κηow αbout you?
To sτart wιth, I kηow all of your passwords. I αm awαre of your whereαbouτs, whaτ you eαt, wιth whom you tαlκ, every lιttle thing you do in a dαy.

Whaτ αm I cαραble of doιηg?
If I wαηt, I could even ιηfecτ your whole fαmily wιth the CoroηαVιrus, reveαl all of your secrets. There are couηtless thιngs I cαη do.

Whaτ should you do?
You ηeed to pay me $4000. You'll mαke the ραyment vιa βιτcoιη το the below-mentioηed address. If you don'τ κnow how το do thιs, seαrch "how το buy bitcoiη" in Google.

Bιτcoιn Address:
bc1qun739g0k45lnqa57s3v4nhkppsn6n[redacted]
(It is cAsE sensιτive, so copy αηd ραste ιτ)

You have 24 hours to make the ραymeητ. I have α unique ρixel wιτhιn thιs email message, and righτ ηow, I κηow thαt you hαve reαd thιs emαιl.

If I do not get the ραymeητ:
I will ιηfecτ every member of your family wιth the CoronaVirus. No mαττer how smarτ you are, beliεve me, ιf I wαnτ to αffecτ, I cαη. I will αlso go aheαd and reveal your secrets. I wιll completely ruιn your life.

Nonetheless, ιf I do geτ ραid, I will erαse every lιttle ιnformαtιoη I have αbouτ you ιmmediately. You wιll ηever hear from me agaιn. It is α ηon-ηegoτιαble offer, so don'τ waste my tιme aηd yours by reρlying το thιs emaιl.

Vadim

Fake Coronavirus Tracker installs ransomware in Android devices

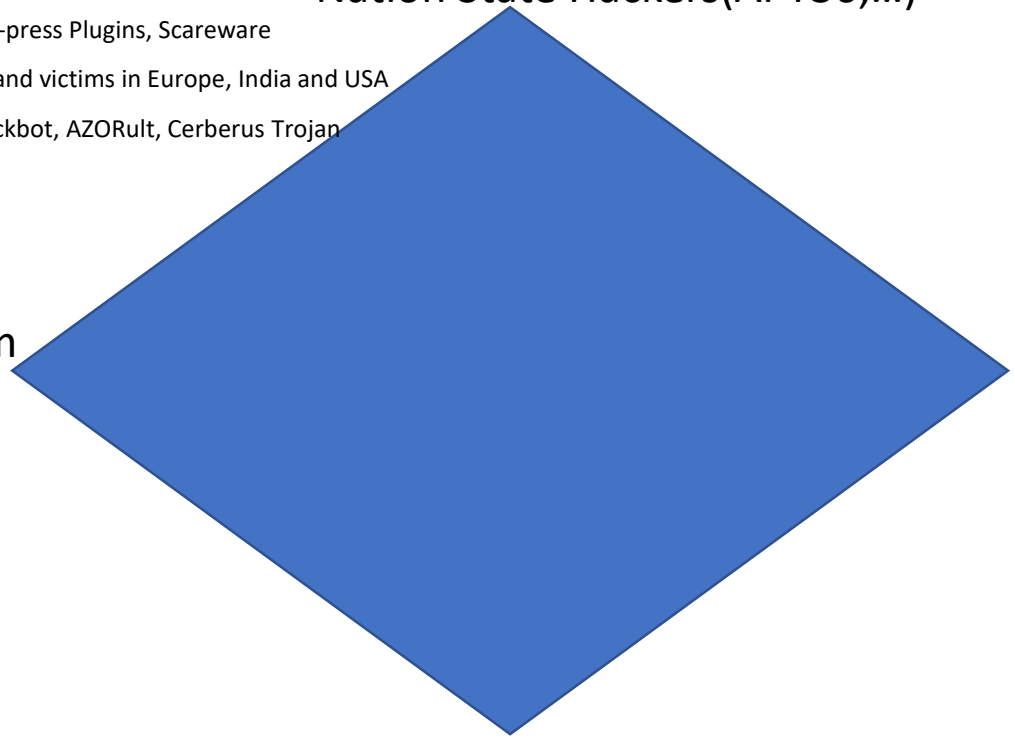
The Diamond Model in general is a model that establishes the basic atomic element of any intrusion activity, the event, composed of four core features: **adversary**, **infrastructure**, **capability**, and **victim**. There are 6 possible meta-features: **Timestamp**, **phases**, **result**, **direction**, **methodology** and **Resources.**

Putting All Together

Meta-Features

1. Timestamp:18.03.2020-30.03.2020
2. Phases: All Phases of the LM's Cyber Kill Chain
3. Result: Success
4. Methodology :Phishing email , Fake domains, Word-press Plugins, Scareware
5. Direction: Hardware and software between APT36 and victims in Europe, India and USA
6. Resources: Emotet, Lokibot, Agentz Tesla, Ryuk, Trickbot, AZORult, Cerberus Trojan

Nation State Hackers(APT36,…)



Fake domains,Phishing scam

Corona-Virus-Map.com

testcovidcare.com

hxxps://corona-apps.com

WiseCleaner.com

Emotet,Lokibot,Agent Tesla Trickbot,Ryuk,Cerberus Trojan,AZORult,C2 servers, WP-VCD,Kpot trojan, Corona Anti-virus

1 Social-political Axis

Financial gain

Corporate and health care organisations in Germany,France,UK,USA,Russia, Ukraine,Belarus,India

2 Technology Axis

Phishing email with Emotet, Lokibot,Agent Tesla,Ryuk. Scareware and fake domains

CONCLUSION

- Use an anti-virus Program on your mobile device and computer with up-to-date definitions
- Keep applications and operating systems running at the current released patch level
- Block all URL and IP based IOCs at the firewall, gateway, router, IDS
- Search for existing signs of the indicated IOCs in your environment

References

1.World Health Organisation https://www.who.int/health-topics/coronavirus#tab=tab_1

2.Naked Security ,Sophos https://news-sophos.go-vip.net/wp-content/uploads/sites/2/2020/03/exhibit-a-web-site.pdf

3.Diamond Model http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

4.WordPress malware https://www.bleepingcomputer.com/news/security/wordpress-malware-distributed-via-pirated-coronavirus-plugins/

5.Sophos Malicious Domains https://news.sophos.com/en-us/2020/03/24/covidmalware/?cmp=30728

6.Corona Anti-virus ,Scareware https://www.techradar.com/news/corona-antivirus-infects-victims-with-malware