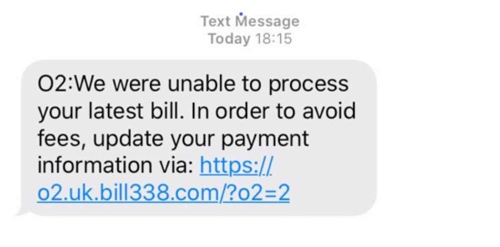
BAMBOO

▶ CYBER ▶ EYES

The Coronavirus continues to lead headlines both on traditional news and in the cyber realm. Many threat actors continue to leverage themes relating to this pandemic in countless campaigns. These lures work exceptionally well as Internet usage is at record levels and curiosity about the virus is at an all-time high. Essentially, the potential victim pool is larger than ever and more likely to fall for such schemes.

We would like to share with you an overview of the weeks news. Whilst you will undoubtedly have heard or even seen other attempts we've tried to capture a few from a variety of mediums you will be taking advantage of.

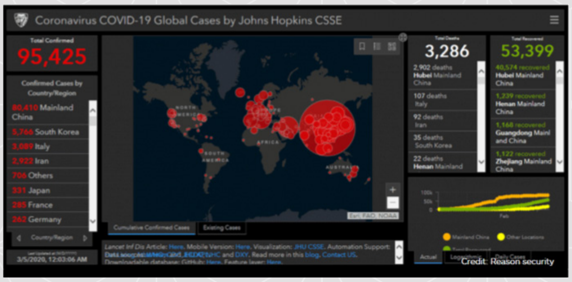
WHAT WE'VE SEEN



Text Message
Today 18:15

O2:We were unable to process your latest bill. In order to avoid fees, update your payment information via: https://o2.uk.bill338.com/?o2=2

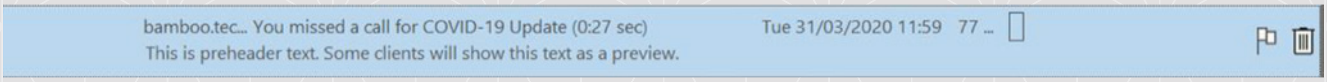
Fake O2 payment texts



Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE
Total Confirmed
95,425
Confirmed Cases by Country/Region
80,410 Mainland China
5,766 South Korea
3,089 Italy
2,922 Iran
706 Others
331 Japan
285 France
262 Germany
Country/Region
3/5/2020, 12:03:06 AM
NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
AUSTRALIA
Esri, FAO, NOAA
Cumulative Confirmed Cases
Existing Cases
Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support:
Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US.
Downloadable database: GitHub: Here. Feature layer: Here.
Total Deaths
3,286
2,902 deaths Hubei Mainland China
107 deaths Italy
92 deaths Iran
35 deaths South Korea
22 deaths Henan Mainland
Total Recovered
53,399
40,574 recovered Hubei Mainland China
1,239 recovered Henan Mainland China
1,168 recovered Guangdong Mainland China
1,122 recovered Zhejiang Mainland China
100k
50k
0
Feb
Mainland China
Other Locations
Total Recovered
Actual
Logarithmic
Daily Cases

Credit: Reason security

COVID-19 spread indicator websites – redirecting to malicious pages



bamboo.tec... You missed a call for COVID-19 Update (0:27 sec) Tue 31/03/2020 11:59 77 ...

This is preheader text. Some clients will show this text as a preview.

Fake Missed call COVID-19 emails

WHAT WE'VE HEARD ABOUT

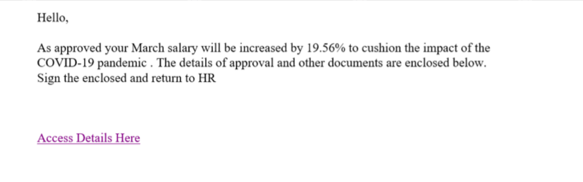
1. General performance issues regarding access to Office 365, and software as a service in general.

2. Salary increase emails with click through links

3. Fake Furlough advice emails with click through links

4. Fake Police SMS giving false information with malicious links

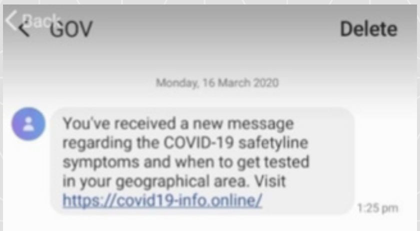
5. Fake COVID-19 'testing' messages



Hello,

As approved your March salary will be increased by 19.56% to cushion the impact of the COVID-19 pandemic . The details of approval and other documents are enclosed below. Sign the enclosed and return to HR

Access Details Here



Monday, 16 March 2020

You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

1:25 pm

For further information or indicators of compromise please email cyber@bamboo.tech

BAMBOO
▶ CYBER ▶ EYES

WHAT WE'VE BEEN MADE AWARE OF

Despite a sizable chunk of the population being left out of work due to the virus, many people have switched to remote work. Furthermore, the quarantine is pushing people to spend more time on Internet-connected devices, especially mobile phones. Our threat intelligence partner has observed two unique mobile-focused campaigns last week aimed at both iOS and Android.

The first campaign targets iOS devices with a new backdoor dubbed LightSpy. The malware allows attackers to execute shell commands and manipulate files. It first emerged as part of a watering hole attack on users in Hong Kong. The campaign uses links posted on multiple forums that supposedly lead to various news stories. The links lead users to actual news sites, but also use a hidden iframe to load and execute malicious code. In addition to executing commands, the malware extracts an array of sensitive data.

Separately, another campaign targets Android users with a Coronavirus-themed app. The app claims to provide a free safety mask, but instead requests permissions to access the user's address book and the ability to view SMS. It then abuses these permissions to spread to the entirety of the victim's contact list. Mobile, which was already a hot target is even more attractive now to would-be threat actors and this trend will almost certainly continue for the foreseeable future.

0DAY – EXPOSED CORONA – PHISHING CAMPAIGN

A new phishing campaign distributes emails purporting to be from a local hospital informing the recipient that they have been exposed to the Coronavirus (COVID-19) and will need to be tested.

Specifically, the emails state that the user has been in contact with a colleague, friend or family member who tested positive for the virus. The email then instructs the user to print the attached **Emergency Contact.xlsm** attachment and bring it to the nearest emergency clinic for testing.

Upon opening the Excel document, it displays a graphic instructing the user to enable macros. If enabled, the document executes malicious macros to download a malware executable. This executable then injects numerous processes into the legitimate Windows msiexec.exe file. This is done to hide the presence of the running malware and potentially evade detection by security programs.

The unidentified malware offers the following capabilities:

Search and possibly steal cryptocurrency wallets
Steals web browser cookies
Collects list of running programs
Looks for open shares on the network
Collects local IP address information

The best way to keep all our businesses safe is to share information regarding both foiled and successful attempts. Please do share any information you may have so that we can share with Bamboos wider business network.

For further information or indicators of
compromise please email cyber@bamboo.tech