BAMBOO
CYBER EYES

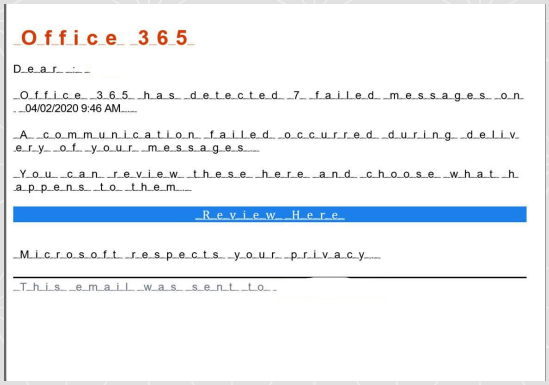
The Coronavirus continues to lead headlines both on traditional news and in the cyber realm. Many threat actors continue to leverage themes relating to this pandemic in countless campaigns. These lures work exceptionally well as Internet usage is at record levels and curiosity about the virus is at an 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

Ransomware attacks stemming from poor password policies.

Successful spear phishing campaigns and attacks coming from lack of security protocols around financial processes.


Office 365

Dear ...

Office 365 has detected 7 failed messages on 04/02/2020 9:46 AM

A communication failed occurred during delivery of your messages.

You can review these here and choose what happens to them.

Review Here

Microsoft respects your privacy

This email was sent to

Office365 phishing

Incoming requests for Multi Factor Authentication have increased sharply in the last few weeks. If you would like to know more about how to protect your business please contact the team at **cyber@bamboo.tech**.

# WHAT WE'VE HEARD ABOUT

## Virtual Meeting Applications Quickly Become a Top Target

Malicious actors are increasingly targeting virtual meeting applications as much of the global workforce embarks on a work-from-home venture amidst the Coronavirus pandemic. One report suggests Skype to be the front runner with over 120,000 suspicious files using its name for both malware and adware.

## Coronavirus-Themed Apps Targeting Android Devices

A new collection of Android apps purport to offer help and info on COVID-19 but instead deliver remote access trojans and other malware. The observed campaign consists of at least 16 different Coronavirus applications, none of which come from the official Google Play Store. This trend is highly likely to continue throughout the duration of the pandemic.

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

BAMBOO
CYBER EYES

# WHAT WE'VE BEEN MADE AWARE OF

## Mobile Spyware

Project Spy is a new potential cyberespionage campaign that infects both Android and iOS devices with spyware. The campaign leverages the ongoing Coronavirus (COVID-19) pandemic as a lure by posing as an app called Coronavirus Updates. The app has only garnered a small number of downloads in Pakistan, India, Afghanistan, Bangladesh, Iran, Saudi Arabia, Austria, Romania, Grenada, and Russia at time of writing. The app's features include:

- Upload GSM, WhatsApp, Telegram, Facebook, and Threema messages
- Upload voice notes, contacts stored, accounts, call logs, location information, and images
- Upload the expanded list of collected device information (e.g., IMEI, product, board, manufacturer, tag, host, Android version, application version, name, model brand, user, serial, hardware, bootloader, and device ID)
- Upload SIM information (e.g., IMSI, operator code, country, MCC-mobile country, SIM serial, operator name, and mobile number)
- Upload wifi information (e.g., SSID, wifi speed, and MAC address)
- Upload other information (e.g., display, date, time, fingerprint, created at, and updated at)

Several previous versions of the malware were also observed. These versions contained similar but fewer spyware functionalities, demonstrating the progression of the app. One of the versions lists the developer name as "concipit1248" in Google Play. Using this name and codes, two related apps also emerged in the Apple App Store.

## Phishing email Trojan

BlueTea Action is a new trojan that spreads via Coronavirus (COVID-19)-themed phishing emails. The email subject line reads "The Truth of COVID-19" and includes a malicious RTF that exploits the CVE-2017-8570 vulnerability. Once the vulnerability is triggered, it executes an .SCT script to evade detection. This script contains multiple layers of obfuscation. BlueTea Action then creates multiple scheduled tasks to establish persistence.

The trojan received several updates since release, ranging from the method of dissemination, obfuscation, and profit modules. Initially the malware spread via EternalBlue exploits, but later evolved in incorporate password bruteforcing and now email worms. The malware remains under active development and distribution.

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