CNS CYBER INTELLIGENCE REPORT

Tactical Update: Latest cyber threats related to Coronavirus, 11th May 2020

Date of Issue: 11/5/2020
Reference Number: TU.11.5.20

Context

The following report provides details of latest known cyber threats related to the coronavirus. The report provides the details of known threats and recommended remediation steps. The link for previous copies of Tactical Updates is here. Please note that any links provided within this report are to external websites which are not controlled by CNS Six Degrees.

Threat Details

1. **Phishing campaign targeting Microsoft Teams** – On 1st May, Abnormal Security reported a phishing campaign that impersonated automated notification emails from Teams, informing the user that they had missed a message from a colleague or had a file sent to them from a colleague. The emails contain links which take users to a fake Microsoft login portal, with the aim of the attack to obtain Microsoft Office 365 login credentials which can be used for further malicious activity[i].

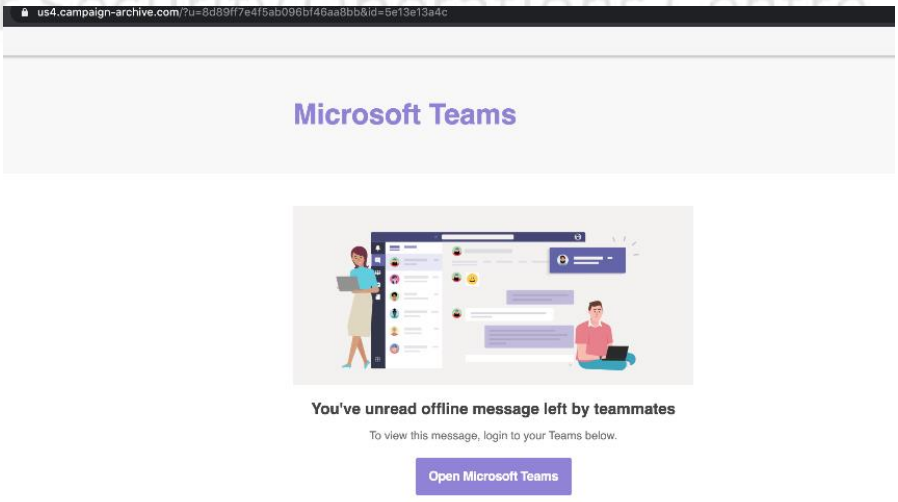

Figure 1 - Screenshot of a phishing Microsoft Teams notification. Note the domain is not a genuine Microsoft address.

2. **Beware key dates in pandemic response due to spikes in cyber-attacks –** CNS has surveyed information related to 75 coronavirus-related cyber campaigns to understand trends in activity. Whilst the data is approximate, it would appear that the launch date of individual campaigns or attacks peaks on key

CNS
A Six Degrees Company

dates of the pandemic response. For example, the largest number of campaigns appeared on 23rd March 2020, the day the UK Government announced the national lockdown. A further peak on 20th April coincided with the UK's Coronavirus Job Retention Scheme accepting applications; the peak was possibly due to cyber criminals attempting to defraud users applying for the financial assistance. Please see Figure 2 for details of the timeline of cyber activity.

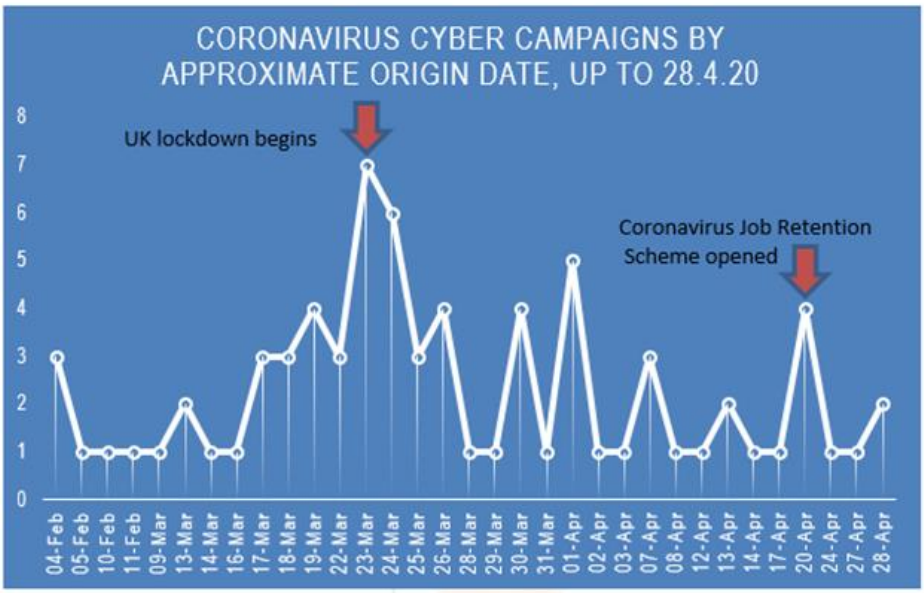

Figure 2 - Numbers of cyber-attacks or campaigns related to coronavirus launched per day based upon data of 75 separate incidents.

Remediation Advice

3. CNS recommends that you make staff aware of the threat of phishing emails related to the coronavirus outbreak and that they should not open any unsolicited emails about the subject from external contacts.

4. The Microsoft Teams phishing attack is designed to obtain Office 365 login details, with the ultimate aim to use these credentials to launch business email compromise (BEC)[1] attacks or ransomware attacks, both of which can cause considerable financial damage to an organisation. CNS recommends that employees are informed they should not log into Office 365 login portals which appear from emails or attachments in emails, as these are likely to be malicious and can lead to credential compromise.

5. CNS recommends that users are aware of the possible increased threat of cyber-attacks during key dates of the UK's pandemic response. For example, beware of smishing (phishing that involves text messages) campaigns that impersonate the UK Government's mass messaging via SMS if there is a policy change related to lockdown.

[i] https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/

[1] Business email compromise is the impersonation of a real member of staff, either through compromised credentials or use of an email address designed to look like the genuine version, to send emails to finance departments and/or clients requesting changes in payments details or scheduled in order to commit fraud.