CRITICAL ADVISORY

Cyber Peace Foundation

PROBLEM NAME:

Unsafe Website with Domain Name formulated with COVID-19/Corona Keyword

DATE(S) ISSUED:

13th April 2020

RISK:

Home Users: Medium

DESCRIPTION:

Cyber fraudsters use COVID-19 pandemic opportunity to spread phishing emails, and malicious links disguise as Corona related information and updates. The suspicious links can be considered under categories of malicious links to spread Malware, Adware and Phishing related links. Identification and suspension of these links would be of utmost priority for a proactive cybersecurity mechanism. With this objective, the set of a malicious URL was identified and processed further. The collection of the malicious links identified are 503 links.

Status of links varies randomly; thus, it is suggestive to keep a regular check on link status. The figures represented here were a reflection of work done in the last five days.

The URLs with COVID-19/Corona keyword were identified and were further investigated for its malicious content. The investigation was carried out using Virus Total online service. The service detects viruses, worms, trojans and other kinds of malicious content in the URLs using antivirus engines and website scanners[2]. The pattern matching mechanism of Virus Total scores suspicious URL/Domain on a scale of 77 where 77 signifies the number of databases of various antivirus scanner and blacklisting services for URL/Domain. The analysis with Virus Total is carried out with respect to the following criteria:

- Serving IP

This is IP address which is marked for latest serving of URL

- Nature of malicious activity

CRITICAL ADVISORY

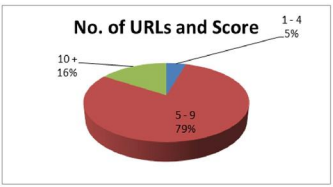
URL is demarcated as either Malicious or Clean by respective databases. If anyone database flags URL as Malicious, then nature of it is mentioned. The categories of nature of malicious URL/Domain involve:

- Phishing
- Malware
- Spam
- Suspicious
- OR a combination of above categories

The complete description of investigated malicious URLs are listed in the excel hosted on the following link:
Link Here*:

The file contains Serving IP, Nature of the malicious activity and Score of each unsafe URLs. The analysis shows(refer Fig. 1) that 79% of URLs score lies between the range of 5 – 9, 16% lie between 10 – 19 range and 5% lie between 1 – 4 range.

Note: Data provided is as of 13th April 2020. Further, this sheet will be updated accordingly for new malicious URLs.



RECOMMENDATIONS:

- Small and Large business/Government offices should blacklist the list website.
- Personal users should block these sites at the system level or the browser level.
- We recommend an action from government authority to block/raise warning against these websites.

EXPLOIT'S POC & REFERENCES:

1. **URLScan.io: https://urlscan.io/**
2. **VirusTotal (Home page): https://www.virustotal.com/gui/home**

CRITICAL ADVISORY

CAUTION:

While you all may be aware of this advisory through other sources. The following advisory is to assist you in effectively mitigating the stated risk and vulnerability. This may not be completed in and by itself, request you to consider your other sources for closure.

REVISION NOTES

Version	Description	Section	Status	Date
1.0	Initial public release	----	Final	2020-Apr-13

RESEARCH TEAM

Cyber Peace Foundation (CPF) https://www.cyberpeace.org/

CPF Center of Excellence @ K J Somaiya COE, Mumbai. https://kjsce.somaiya.edu/kjsce/