البنك المركزي المصري

CENTRAL BANK OF EGYPT

مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المصرفي

Egyptian Financial Computing Incident Response

Report Summary

COVID-19 Pandemic Exploited by Malicious Cyber Actors

Report Summary

⚠ Critical	⚠ High	⚠ Medium	⚠ Informative

Report ID & Issuance Date:	5/2020	**Reported Date:**	15 April 2020
Alert Title:	COVID-19 Pandemic Exploited by Malicious Cyber Actors		
Severity:	⚠	Medium	
Description:	Security researchers from the United States Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) provides information on exploitation by cybercriminals and Advanced Persistent Threat (APT) groups of the current coronavirus disease (COVID-19) global pandemic. At the same time, the surge in remote working has increased the use of potentially vulnerable services exposed to the internet. APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams emails and phishing attacks.		
Analysis:	APT groups masquerade as trusted entities using the COVID-19 pandemic as part of their cyber-security operations. In addition, Cybercriminals are using the pandemic for commercial gain via deploying a variety of ransomware and other malwares. Threats observed by both APT groups and cybercriminals include: • Large amounts of Phishing attacks using the subject of coronavirus, COVID-19, Coronavirus-Update or Coronavirus-outbreak in your city as a lure for credentials theft or malware distribution. • Registration of new domain names containing wording related to Coronavirus or COVID-19. • Attacks against infrastructure by exploiting unpatched exposed services to internet like unsecured RDP endpoints, VPN, and Exchange servers...etc. This report includes a non-exhaustive list of Indicators of Compromise (IOCs) for detection as well as mitigation advices.		

Vulnerabilities Exploited:	N/A
Indicator of Compromise (IOCs):	Attached "COVID-19 IOCs"
Mitigations:	• Antivirus and monitoring tools should be updated regularly. • Search for existing signs of the indicated IoCs in your environment. • Block the mentioned IoCs at organization's security devices. • Implement filters at the email gateway to filter out emails with known email spam indicators. • Recommended to use Endpoint detection and response (EDR) tool. • Implement cyber-security awareness training sessions for staff so that they will know the risk associated with the cyber security risks especially phishing attack and how to distinguish it. • Recommended to examine organization employees' cyber-security awareness by simulating a spear-phishing campaign. • Recommended to use encrypted, trusted and license products for web conference meetings and avoid free products. • Any service open to the public internet needs to be up-to-date on patches level and protected by preventative controls (such as endpoint protection software), and actively monitored for anomalous login and other abnormal behavior .
References:	• https://www.us-cert.gov/ncas/alerts/aa20-099a