Examples of COVID-19 Threats: Summary of Attacks

APT groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and "hack-and-leak" operations.

Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cybercriminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure,
- Malware distribution, using coronavirus- or COVID-19- themed lures,
- Registration of new domain names containing wording related to coronavirus or COVID-19, and
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action. These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
    - For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install "CovidLock" ransomware on their device.[1]

- Open a file (such as an email attachment) that contains malware.
    - For example, email subject lines contain COVID-19-related phrases such as "Coronavirus Update" or "2019-nCov: Coronavirus outbreak in your city (Emergency)"

To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with "Dr." in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other emails purport to be from an organization's human resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with coronavirus- or COVID-19-related themes, such as "President discusses budget savings due to coronavirus with Cabinet.rtf."