Security Tips

Mississippi Department of Information Technology Services
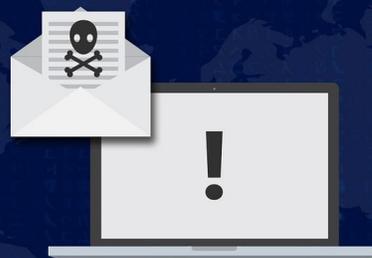
Cyber Threat Actors Expected to Leverage Coronavirus Outbreak

From the desk of Thomas F. Duffy, MS-ISAC Chair

For More Information:

FTC Warns of Ongoing Scams Using Coronavirus Bait

Cyber threat actors (CTA) leverage interest during public health threats and other high-profile events in order to conduct financial fraud and disseminate malware. We expect that this trend will continue with the emergence of new and recycled scams involving financial fraud and malware related to the coronavirus outbreak.

Malicious actors are likely to post links to fake charities and fraudulent websites that solicit donations for relief efforts or deliver malware. The MS-ISAC observed similar scams and malware dissemination campaigns in response to previous high-profile events including Hurricane Harvey, the Boston Marathon bombing, the Royal Wedding, and the Tennessee wildfires. Its highly likely that more scams and malware will follow over the course of the response period. Internet users should exercise caution before opening related emails, clicking links, visiting websites, or making donations to coronavirus relief efforts.

Warning Signs

As of February 1, 2020, the MS-ISAC had observed the registration of names containing the phrase "coronavirus." The majority of these new domains include a combination of the words "help," "relief," "victims," and "recover." Most of the domains appear to be currently under development. However, as a few appear malicious and the domains themselves appear suspect, these domains should be viewed with caution. More domain registrations related to the coronavirus are likely to follow in the coming days.

The potential of misinformation during times of high-profile global events and public health threats is high and users should verify information before trusting or reacting to posts seen on social media. Malicious actors often use social media to post false information or links to malicious websites. The MS-ISAC observed similar tactics in the days following Hurricane Irma's landfall and other natural disasters.

It is likely that CTAs will also capitalize on the outbreak to send phishing emails with links to malicious websites advertising relevant information. It is possible these websites will contain malware or be phishing websites requesting login credentials. Other malicious spam will likely contain links to, or attachments with, embedded malware. Victims who click on links or open malicious attachments risk compromising their computer to malicious actors.

How to Avoid Being the Victim

The MS-ISAC recommends that users adhere to the following guidelines when reacting to high-profile events, including news associated with the coronavirus, and solicitations for donations:

- Users should exercise extreme caution when responding to individual pleas for financial assistance such as those posted on social media, crowd funding websites, or in an email, even if it appears to originate from a trusted source.
- Be cautious of emails or websites that claim to provide information, pictures, and videos.
- Do not open unsolicited (spam) emails or click on the links or attachments in those emails.
- Never reveal personal or financial information in an email or to an untrusted website.
- Do not go to an untrusted or unfamiliar website to view the event or information regarding it.
- Malicious websites often imitate a legitimate website, but the URL may use a variation in spelling or a different domain (e.g., .com vs .org).

The MS-ISAC recommends that technical administrators adhere to the following guidelines when reacting to and protecting their networks and users during high-profile events, including news associated with coronavirus:

- Warn users of the threats associated with scams, phishing, and malware associated with high-profile events and train users about social engineering attempts.
- Implement filters at your email gateway to filter out emails with known phishing attempt indicators and block suspicious IPs at your firewall.
- Flag emails from external sources with a warning banner.
- Implement DMARC to filter out spoofed emails.

Provided By

MS-ISAC
Multi-State Information

STOP | THINK
CONNECT