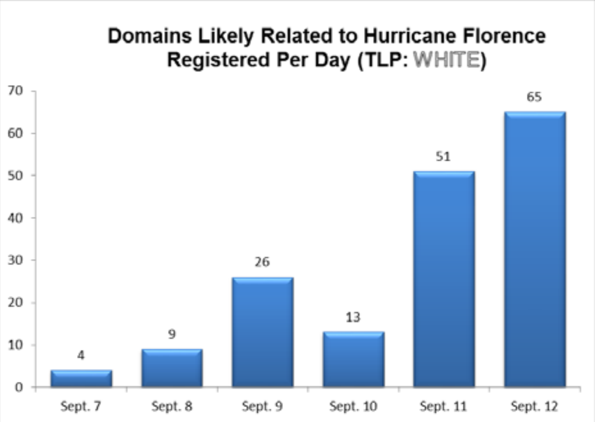
Cyber Intel Advisory

September 14, 2018 – IA2018-0338

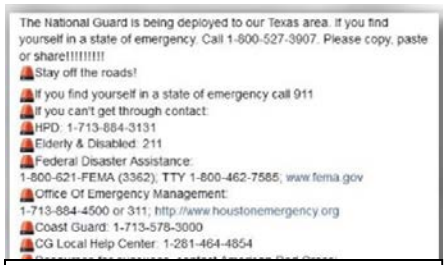
Cyber Threat Actors Expected to Leverage Major Storms for Fraud

TLP: WHITE Malicious actors leverage public interest during natural disasters and other high profile events in order to conduct financial fraud and disseminate malware. The landfalls and impending landfalls of Hurricanes Florence, Isaac, and Helene, Tropical Storm Olivia, and Typhoon Mangkhut will highly likely propel the emergence of new and recycled scams involving financial fraud and malware.

TLP: WHITE Malicious actors often post links to fake charities and fraudulent websites that solicit donations for victims of the hurricane or deliver malware. The Multi-State Information Sharing and Analysis Center (MS-ISAC) previously observed similar scams and malware dissemination campaigns in response to high profile events including the Boston Marathon bombing, Hurricane Harvey, and the Tennessee wildfires. It is highly likely that more scams and malware will follow over the course of the recovery period, so Internet users need to exercise caution before opening related emails, clicking links, visiting websites, or making donations to relief efforts.



- From September 6-11, 2018, the MS-ISAC observed an increase in registered domains likely related to Hurricane Florence. The most recently registered domains include the words, “claims,” “compensation,” “lawyers,” “relief,” and “funds,” which could indicate the domains use in possible scams or other malicious activity, so they should be viewed with caution. It is likely that these domain registrations will continue, especially after Hurricane Florence makes landfall. We believe that these domain registrations will also likely occur for the other storms.
- During and after disasters, the potential of misinformation disseminated by malicious actors is high and users should verify information before reacting to posts seen on social media. Some of these posts may go viral, as did the one to the right during Hurricane Harvey, which hit Houston, Texas, in 2017. In this example, the number provided for the National Guard is incorrect and when dialed, connects to an insurance company. The insurance company corrects the misinformation and instructs the caller to contact 9-1-1.


The National Guard is being deployed to our Texas area. If you find yourself in a state of emergency. Call 1-800-527-3907. Please copy, paste or share!!!!!!!!!
🚨Stay off the roads!
🚨If you find yourself in a state of emergency call 911
🚨If you can't get through contact:
🚨HPD: 1-713-884-3131
🚨Elderly & Disabled: 211
🚨Federal Disaster Assistance:
1-800-621-FEMA (3362); TTY 1-800-462-7585; www.fema.gov
🚨Office Of Emergency Management:
1-713-884-4500 or 311; http://www.houstonemergency.org
🚨Coast Guard: 1-713-578-3000
🚨CG Local Help Center: 1-281-464-4854

(TLP: WHITE) Viral scam targeting Hurricane Harvey victims

- It is highly likely that malicious actors will also capitalize on this disaster to send phishing emails with links to malicious websites advertising relevant information, pictures, and videos, but containing phishing webpages or malware. Other phishing emails are highly likely to contain links to, or attachments with, embedded malware. Victims who click on links or open malicious attachments risk compromising their computer.

USER RECOMMENDATIONS:
TLP: WHITE The MS-ISAC recommends that users adhere to the following guidelines when reacting to high profile events, including news associated with the disasters 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. When making donations, users should consult the Federal Trade Commission Consumer Information website for guidance or the National Voluntary Organizations Active in Disaster website.
- 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 site, but the URL may use a variation in spelling or a different domain (e.g., .com vs .org) so ensure the link goes to the correct website.

TECHNICAL RECOMMENDATIONS:
TLP: WHITE The MS-ISAC recommends that technical administrators adhere to the following guidelines when reacting to high profile events, including news associated with any of these disasters, and solicitations for donations:

- Issue warnings to users about potential scams, implement filters on emails, block suspicious IP addresses and domains at your firewall and on your webserver proxy, and flag emails from external sources with a warning banner
- Use antivirus programs on clients and servers, with automatic updates of signatures and software.
- Apply appropriate patches and updates immediately after appropriate testing.

More information regarding emergency preparedness for cyber infrastructure is available in the associated MS-ISAC Security Primer.

(U) TLP: WHITE The information in this document is current as of September 13, 2018. The information provided above is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. Organizations have permission and are encouraged to brand and redistribute this advisory in whole for educational, non-commercial purposes. The MS-ISAC is interested in your comments - an anonymous feedback survey is available.

Citations and more information regarding potential threats are available by contacting:

Carolyn Field
Communications Supervisor – CIRMA
203-498-3032 · cfield@ccm-ct.org

MS-ISAC
866-787-4722 · SOC@cisecurity.org