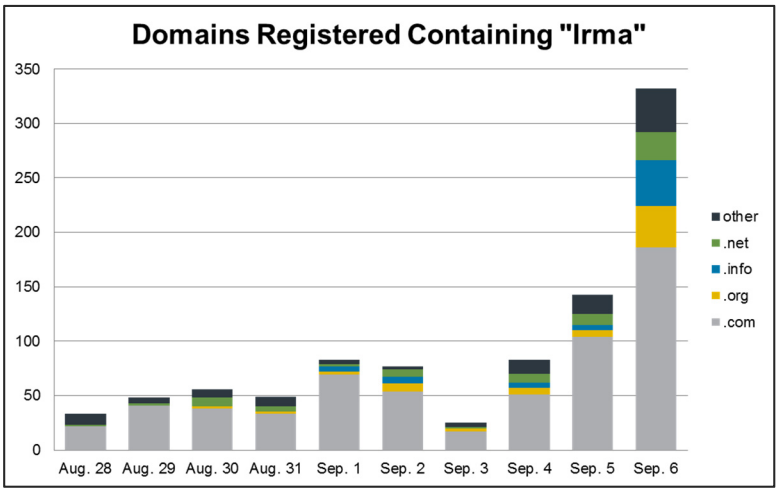
Cyber Intel Advisory
September 8, 2017 – IA2017-0541

Cyber Threat Actors Expected to Leverage Hurricane Irma

TLP: WHITE Cyber threat actors (CTA) leverage public interest during natural disasters 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 Hurricane Irma.

TLP: WHITE Malicious actors are likely to post links to fake charities and fraudulent websites that solicit donations for victims of the hurricane 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, 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 should exercise caution before opening related emails, clicking links, visiting websites, or making donations to Hurricane Irma relief efforts.

- As of September 7, 2017, the MS-ISAC had observed the registration of more than 743 domain names containing the phrase "Irma." The majority of these new domains include a combination of the words "help," "relief," "victims," "recover," "claims", or "lawsuits." 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 Hurricane Irma are likely to follow in the coming days.



- The potential of misinformation during times of disaster 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 Harvey's landfall.
- It is likely that CTAs will also capitalize on this disaster to send phishing emails with links to malicious websites advertising relevant information, pictures, and videos. 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.

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 Hurricane Irma, 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 National Voluntary Organizations Active in Disaster website at https://www.nvoad.org for a list of vetted disaster relief organizations.
- 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).

TECHNICAL RECOMMENDATIONS:
TLP: WHITE 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 Hurricane Irma:

- 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.
- Consider forming a working group with representatives from federal and local law enforcement to help combat Hurricane Irma related Internet fraud.

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. For more information regarding potential cyber threats please visit the Center for Internet Security website at CISecurity.org.

(U) TLP: WHITE The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.

(U) TLP: WHITE The information in this document is current as of September 8, 2017. Citations and more information regarding potential cyber threats are available by contacting:

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