Cyber Intel Advisory
May 14, 2018 – IA2018-0223

Royal Wedding Scams Likely Pose Risks to SLTT Government Networks

TLP: WHITE Malicious actors leverage public interest during high-profile events, such as the May 19, 2018, U.K. royal wedding between Prince Harry and Meghan Markle, in order to conduct financial fraud and disseminate malware. The associated scams, spam, and malware pose a risk to state, local, tribal, and territorial (SLTT) government networks when employees view content or open emails pertaining to the royal wedding while on an SLTT government system.

TLP: WHITE It is likely that malicious actors will leverage public interest to conduct scams and disseminate malware leading up to and immediately following the wedding so Internet users need to exercise caution before opening emails, clicking links, or visiting websites related to the royal wedding. Previously, malicious actors took advantage of heightened public interest surrounding the 2011 royal wedding of Prince William, the birth of Princes George and Louis and Princess Charlotte, as well as other high profile events such as Hurricane Harvey and the Boston Marathon bombing, to establish fake websites, distribute spam, and disseminate malware.

- It is likely that malicious actors will capitalize on the public interest surrounding the royal wedding to send phishing emails that contain malicious attachments or links that advertise relevant information, pictures, and videos of the royal wedding, but are designed to steal credentials or infect users with malware. Victims who open malicious attachments or navigate to embedded links risk compromising their computer to malicious actors. After the birth of Prince George, malicious actors sent phishing emails and posted links on social media purporting to contain detailed information about the new Prince. Some emails contained links to an exploit kit.
- The Multi-State Information Sharing and Analysis Center (MS-ISAC) observed the registration of malicious domains in the lead up to and immediately after previous high profile events. These domains frequently include the year of the event in the domain name, words like “live” and/or “stream,” and are registered under various top level domains (TLDs) such as “.com,” “.info,” and “.net.” It is likely that a similar trend of domain name registrations will occur as the date of the wedding draws nearer. Domains containing keywords that are relevant to the royal wedding should be viewed with extreme caution.
- With the increasing popularity of cryptocurrency mining, it is likely that some websites will advertise information related to the royal wedding to hijack the processing power of visitor’s machines to mine for cryptocurrency. While this activity is not necessarily malicious, cryptocurrency mining causes users’ machines to perform slower and consume more resources than usual, which is likely to have a detrimental effect on SLTT government operations.
- The potential of misinformation during such events is high and users should verify information before reacting to posts seen on social media, blogs, or other sites. Malicious actors use social engineering techniques such as posting interesting, yet misleading information, in hopes of generating enough interest or creating a strong emotional response such that users abandon caution and open the malicious links.

USER RECOMMENDATIONS:

TLP: WHITE The MS-ISAC recommends that users adhere to the following guidelines when reading about or reacting to high-profile events, including news associated with the royal wedding:

- Be cautious of emails or websites that claim to provide information, pictures, and videos of the royal wedding.
- 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). This practice is known as typosquatting.
- If a workstation is performing slower than usual, particularly after browsing the web, users should close and restart their web browser. This will kill any web based cryptocurrency miners that may be running on the machine. If the system continues to perform slowly, immediately notify the information technology department.

TECHNICAL RECOMMENDATIONS:

TLP: WHITE The MS-ISAC recommends that technical administrators adhere to the following guidelines when dealing with high-profile events, including news associated with the royal wedding:

- Use this opportunity to remind users that they should only use official trusted sources to view news and to view emails, social media postings, and other content related to the royal wedding with extreme skepticism. Similarly, remind users not to click on links in emails or on social media that they receive regarding the event.
- Implement filters at your email gateway to filter out emails with known phishing indicators and block suspicious IPs at your firewall.
- Flag emails from external sources with a warning banner.
- Ensure anti-virus software is running and up-to-date with the latest malware definitions.

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 May 14, 2018. Citations and more information regarding potential cyber threats are available by contacting:

NH-CIC
603-227-0087 · NH-CIC@doit.nh.gov
https://www.nh.gov/doit/cybersecurity/index.htm

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