NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Cyber Alert

TLP:WHITE

Product No. 2020-08-002

HSEC-1 | NTIC SIN No. 2.5

August 4, 2020

NTIC CYBER CENTER ALERT

Cyber Threat Actors Exploit Open Redirect Vulnerabilities on Government Websites

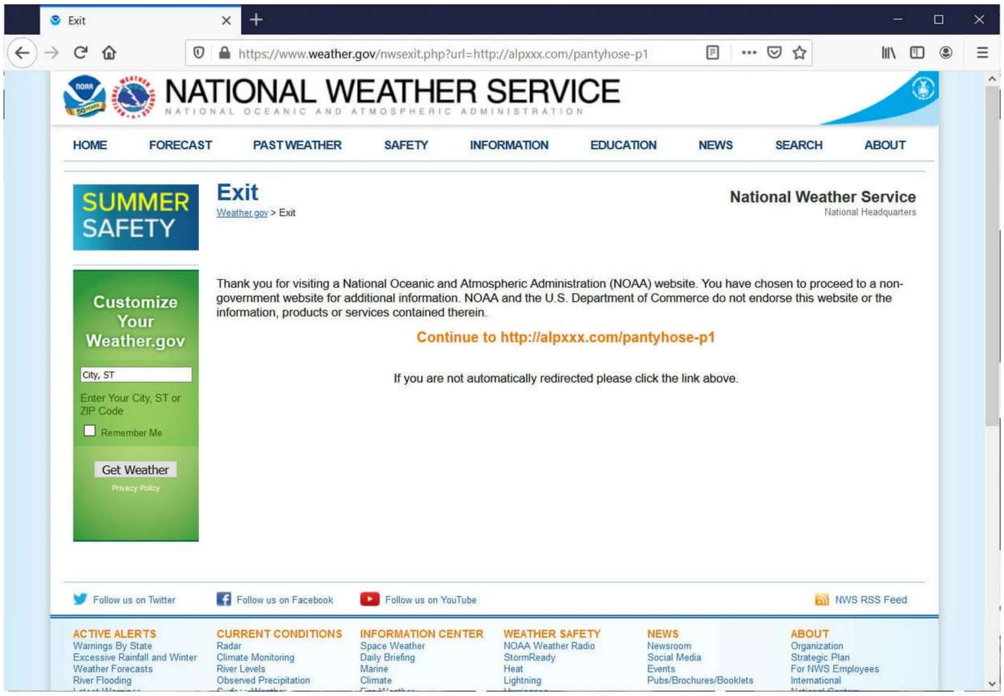
NTIC Cyber Center members,

This alert is being provided for informational purposes and for potential use to protect systems, networks, and data against this cyber threat at the sole discretion of recipients. As the cyber threat landscape is ever-evolving and attribution can be difficult, the NTIC Cyber Center makes no guarantees of the accuracy of this information during and after the dissemination of this alert as indicators of compromise (IoCs) and adversary tactics, techniques, and procedures (TTPs) may change. Recipients are urged to use caution before implementing any changes to systems, software, and procedures.

SUMMARY

Unknown threat actors are currently leveraging open redirect vulnerabilities present on various government websites to send unsuspecting victims to websites featuring adult content. Open redirect vulnerabilities are weaknesses or misconfigurations in web applications that allow for unvalidated redirects or forwards. These threat actors use search engine optimization (SEO) tactics to make their malicious open redirects appear on search engine listings, making it appear as though adult content is hosted on government websites. While government system administrators have been removing malicious open redirects, threat actors have continued to generate new ones. Exploited government domains include those associated with the National Weather Service, the Dwight D. Eisenhower Memorial, the Federal Communications Commission, and the Colorado Department of Higher

Education.



Exit

Weather.gov > Exit

National Weather Service
National Headquarters

Thank you for visiting a National Oceanic and Atmospheric Administration (NOAA) website. You have chosen to proceed to a non-government website for additional information. NOAA and the U.S. Department of Commerce do not endorse this website or the information, products or services contained therein.

Continue to http://alpxxx.com/pantyhose-p1

If you are not automatically redirected please click the link above.

(screenshot of open redirect exploitation - image source: BleepingComputer)

RECOMMENDATIONS

The NTIC Cyber Center recommends website administrators review the Bleeping Computer article here for more information about this campaign. We also recommend reviewing the NTIC Cyber Center's Cyber Advisory titled Open Redirect Vulnerabilities Facilitate Malicious Cyber Activity for more information about this type of attack and recommended mitigation strategies. As open redirect vulnerabilities can be used to conduct phishing attacks as well as distribute malware to victims, we recommend website administrators identify and mitigate any open redirect vulnerabilities present on their websites as soon as possible.

The information contained in this alert is designated TLP:WHITE, subject to standard copyright rules, and may be distributed without restriction.

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: This NTIC Cyber Center Cyber Alert is provided for informational purposes only. The NTIC Cyber

Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.