Cybersecurity Alert for DNS Tampering	Cyber Alert
Criticality:Red:Medium-High	**01/24/2019 9:30 AM**

Summary	The Department of Homeland Security issued an Emergency Directive on DNS infrastructure tampering. DHS is tracking a series of incidents involving DNS tampering, so audit your domain name system (DNS) records and implement the safeguards described in the DHS directive to protect them.
Criticality	Criticality is ***medium-high***, based on current events and potential for harm. Impact from an incident is high. Likelihood for enterprises in critical infrastructure sectors is medium-high. Likelihood for small-medium businesses is medium-low. Note: See below for criticality criteria.
Definition: DNS	DNS is like the "telephone book" of the internet. When you type www.cnn.com into your browser address bar, DNS translates that into the destination's IP address so you're "magically" connected to the correct website. If somebody messes with or hijacks your systems' DNS records, they can redirect you to malicious websites without your knowledge. They can also redirect email and other network traffic.
Details	The DHS Directive, ED19-01 requires all federal civilian agencies to take the actions below by February 5, 2019. These are good recommendations for all organizations. 1. Audit DNS records 2. Change DNS account passwords 3. Add multi-factor authentication (MFA) on DNS accounts, and 4. Monitor Certificate Transparency logs to ensure authenticity of certificate requests. DHS Statement on ED19-01: https://cyber.dhs.gov/ed/19-01/

Tools	There are online tools to help monitor Certificate Transparency logs for any changes to certificates issued for your organization. Google, for example, has a tool to search Certificate Transparency logs that shows all third-party CA-issued certificates for a specific domain. This is useful to see if anyone else has managed to obtain a third-party-signed certificate for a domain that they've hijacked: These are the known (and trusted by Google Chrome) log operators: http://www.certificate-transparency.org/known-logs This is a list of public Certificate Transparency logs (and the list is API-friendly): https://www.gstatic.com/ct/log_list/all_logs_list.json
For More Info	For more information, see US-CERT: https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign FireEye: https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html Cisco Talos: https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
To Report Suspicious Activity	Please report potential, suspected, and/or confirmed cyber threats to the ACTIC. Provide known or suspected • Threat/attack method • Indicators of compromise • Adversary(ies) • Impact, and • Any other threat actor characteristics. Note: The ACTIC shares victims' applicable critical infrastructure sector and scale of operations (national, regional, state, or local level). ***The ACTIC does not share any identifying information without the victim's consent.*** Please report suspicious activity to the ACTIC via: • http://www.azactic.gov/Tips/ • ACTIC@AZDPS.GOV • (602)644-5805 or (877) 2 S A V E A Z (272- 8329)

Criticality Criteria	Listed below is a general description of the criticality rating. The rating is subjective based on information currently known and the analyst's experience. • High / Red: The potential incident may impact or breach critical business, systems, and/or services without immediate intervention. There may also be indications that an attack is currently in process. • Medium / Yellow: The potential incident does not place an organization's business, systems, and/or services in immediate risk but may pose an unacceptable risk if not addressed in a timely fashion. • Low / Green: The potential incident does not pose unacceptable risk but may indicate trends or patterns that might suggest a future impact. • Informational / White: There no current potential incident. Information is for awareness.
Disclaimer	This alert contains raw intelligence that has not been analyzed. It is provided for your situational awareness to help improve Arizona's cyber resiliency. While this document may mention vendors' products and services, the ACTIC does not recommend or endorse any specific ones.