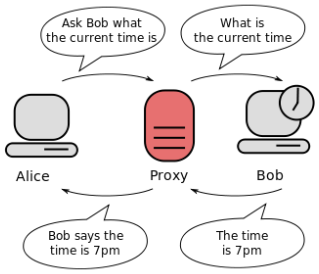
Cybersecurity Advisory — Russia Hacking Network Devices **Criticality:Medium:Yellow:**	**Cyber Advisory** **4/20/2018 5:00 PM**
Summary	Earlier this week, the United States and Britain issued a joint cyber alert, saying that Russian government-backed hackers have been targeting routers and other networking equipment. According to US and UK intelligence agencies, Russia has methodically targeted "network infrastructure devices such as routers, switches, firewalls, network intrusion detection systems" since 2015. Russia's goals are to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operation (attacks).
Criticality	Criticality is ***medium***, based on current events and potential for impact. Note: See below for criticality descriptions.
Why Target Network Devices	According to chief Homeland Security cyber official Jeanette Manfra, "once you own the router, you own the traffic traversing the router." Network devices are often easy targets. Manufacturers build and distribute network devices with exploitable services turned on to make installing and running the devices easier. Many times, the owners and operators of network devices do not change vendor default settings, harden them for operations, or perform regular patching. Internet Service Providers (ISPs) may not promptly replace equipment on a customer's property when that equipment is no longer supported by the manufacturer or vendor.
Recommended Actions — Should You Panic?	No — don't panic. While governments, businesses, and critical-infrastructure providers are the main targets, there are a couple actions you should take: • Change your router password. For instructions, see "References" far below for some how-to articles, check your router manufacturer's website, or contact your ISP. • Change default passwords on any and all internet-connected devices, like your home security system, smart refrigerator, and smart TV.

Definition: Network Devices	There are all different types of network devices. Here are some of the most common. • Router — A networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the internet. At home, a router generally sits between your computer and the cable outlet. • Switch — A device that connects devices together on a computer network to receive, process, and forward data to the destination device. • Bridge — A device that connects multiple network segments. • Proxy server — A computer network service that allows clients to make indirect network connections to other network services.  • Firewall — A piece of hardware or software put on the network to prevent some communications forbidden by the network policy. A firewall typically establishes a barrier between a trusted, secure internal network and another outside (generally untrusted) network, such as the internet. • Network address translator (NAT) — A network service (provided as hardware or as software) that converts internal to external network addresses and vice versa.
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 Descriptions	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.
References	https://www.us-cert.gov/ncas/alerts/TA18-106A https://arstechnica.com/tech-policy/2018/04/russian-hackers-mass-exploit-routers-in-homes-govs-and-infrastructure/ https://www.zdnet.com/article/russian-hacker-warning-how-to-protect-yourself-from-network-attacks/ https://www.lifewire.com/how-to-change-your-wireless-routers-admin-password-2487652 https://www.lifewire.com/how-to-change-your-wireless-routers-admin-password-2487652