THE COMPUTER CORNER

No. 243: Keep Your Eyes Open

Stan Kaplan, WB9RQR 715 N. Dries Street Saukville, WI 53080-1664
(262) 268-1949 wb9rqr@att.net

This is just a portion of an email sent to me in April using the GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT), 245 Murray Lane SW. Bldg 410, Washington, DC 20598, (888) 282-0870. You can get the original email, complete, at www.us-cert.gov. Remember, I have left out a considerable part and edited the remainder, all in the interest of brevity. At least you should scan this shortened document and think about what you can do to prevent yourself from being targeted.

TA18-106A: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices.
Written by the U.S. Department of Homeland Security US-CERT, National Cyber Awareness System: 4/16/2018

Overview: This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC). This TA provides information on the worldwide cyber exploitation of network infrastructure devices (e.g., router, switch, firewall, and network-based intrusion detection system (NIDS) devices) by Russian state-sponsored cyber actors. Targets are primarily government and private-sector organizations, critical infrastructure providers, and the Internet service providers (ISPs) supporting these sectors. This report contains technical details on the tactics, techniques, and procedures (TTPs) used by Russian state-sponsored cyber actors to compromise victims. Victims were identified through a coordinated series of actions between U.S. and international partners. This report builds on previous DHS reporting and advisories from the United Kingdom, Australia, and the European Union. This report contains indicators of compromise (IOCs) and contextual information regarding observed behaviors on the networks of compromised victims. FBI has high confidence that Russian state-sponsored cyber actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations. The current state of U.S. network devices—coupled with a Russian government campaign to exploit these devices—threatens the safety, security, and economic well-being of the United States.

The purpose of this TA is to inform network device vendors, ISPs, public-sector organizations, private-sector corporations, and small office home office (SOHO) customers about the Russian government campaign, provide information to identify malicious activity, and reduce exposure to this activity.

Description

Since 2015, the U.S. Government received information from multiple sources—including private and public-sector cybersecurity research organizations and allies—that cyber actors are exploiting large numbers of enterprise-class and SOHO/residential routers and switches worldwide. The U.S. Government assesses that cyber actors supported by the Russian government carried out this worldwide campaign. These operations enable espionage and intellectual property that supports the Russian Federation's national security and economic goals.

Legacy Protocols and Poor Security Practice

Russian cyber actors leverage legacy or weak protocols and service ports associated with network administration activities. Cyber actors use these weaknesses to:

…identify vulnerable devices;

…extract device configurations;
…map internal network architectures;
…harvest login credentials;
…masquerade as privileged users;
modify
……device firmware,
……operating systems,
……configurations; and
…copy or redirect victim traffic through Russian cyber-actor-controlled infrastructure.

Additionally, Russian cyber actors could potentially modify or deny traffic traversing through the router.

Russian cyber actors do not need to leverage zero-day vulnerabilities or install malware to exploit these devices. Instead, cyber actors take advantage of the following vulnerabilities:

…devices with legacy unencrypted protocols or unauthenticated services,
…devices insufficiently hardened before installation, and
…devices no longer supported with security patches by manufacturers or vendors (end-of-life devices).

Own the Router, Own the Traffic. For example, **a**n actor controlling a router between Industrial Control Systems – sensors and controllers in a critical infrastructure—such as the Energy Sector—can manipulate the messages, creating dangerous configurations that could lead to loss of service or physical destruction. Whoever controls the routing infrastructure of a network essentially controls the data flowing through the network.

Network Devices—Often Easy Targets. Once installed, many network devices are not maintained at the same security level as other general-purpose desktops and servers. The following factors can also contribute to the vulnerability of network devices:
…Few network devices run antivirus, integrity-maintenance, and other security tools that help protect.
…Manufacturers build and distribute network devices with exploitable services just because they are designed for ease of installation, operation, and maintenance.
…Owners and operators of network devices often do not change vendor default settings or harden them for operations or perform regular patching.
…Internet Service Providers (ISPs) often do not replace equipment on a customer's property when the manufacturer or vendor no longer supports that equipment.

Impact

Russian state-sponsored cyber actors have conducted both broad-scale and targeted scanning of Internet address spaces. Such scanning allows these actors to identify enabled Internet-facing ports and services, conduct device fingerprinting, and discover vulnerable network infrastructure devices.

Legitimate user masquerade is the primary method by which these cyber actors exploit targeted network devices. For the most part, cyber actors can easily obtain legitimate credentials, which they then use to access routers. Organizations that permit default or commonly used passwords, have weak password policies, or permit passwords that can be derived from credential-harvesting activities, allow cyber actors to easily guess or access legitimate user credentials.

General Mitigation

Here is what those of us who use, but do not manage networks can do: Immediately change default passwords such as those found in routers when you buy them. Change your other passwords at least once every year, and make the passwords strong (8 characters, upper and lower case, some numbers, and symbols.
Do not reuse the same password across multiple devices; each device should have a unique password.
Happy Computing! Stan