Operational Collaboration Through Global Partnerships

Cybersecurity requires nations to work across borders to share information and work together to strengthen defenses against global threats. Given the volatile threat landscape, CISA and our interagency and international partners have released cybersecurity advisories to warn organizations about cybersecurity threats and provide mitigation guidance against known vulnerabilities. CISA is committed to working with our international allies to build capacity and strengthen our ability to globally defend against cyber incidents, ultimately, enhancing critical infrastructure security and resilience for all.

JOINT ADVISORIES:

- CISA, FBI, NSA, and International Partners Warn Organizations of Top Routinely Exploited Cybersecurity Vulnerabilities

  On April 27, CISA along with the National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) issued a joint Cybersecurity Advisory on the common vulnerabilities and exposures (CVEs) frequently exploited by malicious cyber actors, including the 15 most commonly exploited of 2021. Malicious cyber actors continue to aggressively target disclosed critical software vulnerabilities against broad target sets in both the public and private sectors. While the top 15 vulnerabilities have previously been made public, this Advisory is meant to help organizations prioritize their mitigation strategies.

- CISA, FBI, NSA, and International Partners Issue Advisory on Demonstrated Threats and Capabilities of Russian State-Sponsored and Cyber Criminal Actors

  On April 20, CISA along with the FBI, NSA, Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), National Cyber Security Centre New Zealand (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) and National Crime Agency (NCA) issued a joint Cybersecurity Advisory on Russian state-sponsored and criminal cyber threats to critical infrastructure that could impact organizations both within and beyond Ukraine. It is the most comprehensive view of the cyber threat posed by Russia to critical infrastructure released by government cyber experts since the invasion of Ukraine in February.

- New Sandworm Malware Cyclops Blink Replaces VPNFilter

  On February 23, CISA along with The United Kingdom's (UK) National Cyber Security Centre (NCSC), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) in the U.S. released a joint Cybersecurity Advisory identifying that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to here as Cyclops Blink. The NCSC, CISA, and the FBI have previously attributed the Sandworm actor to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Centre for Special Technologies (GTsST).

- CISA, FBI, NSA and International Partners Issue Advisory on Ransomware Trends from 2021

  On February 9, CISA along with the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) issued a joint Cybersecurity Advisory outlining the growing international threat posed by ransomware over the past year. The advisory also lays out mitigations to help network defenders reduce their risk of compromise, appropriate responses to ransomware attacks, and key resources from each respective cyber agency.

- CISA, FBI, NSA and International Partners Issue Advisory to Mitigate Apache Log4J Vulnerabilities

  On December 22, 2021, CISA along with the FBI, NSA, the Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), Computer Emergency Response Team New Zealand (CERT NZ), New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) issued a joint cybersecurity advisory with technical details, mitigations, and resources to address known vulnerabilities in the Apache Log4j software library. This advisory provides critical guidance that any organization using products with Log4j should immediately implement.

- Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities

  This joint Cybersecurity Advisory released on November 17, 2021 was the result of an analytic effort among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC) to highlight ongoing malicious cyber activity by an advanced persistent threat (APT) group that FBI, CISA, ACSC, and NCSC assess is associated with the government of Iran. FBI and CISA have observed this Iranian government-sponsored APT group exploit Fortinet vulnerabilities since at least March 2021 and a Microsoft Exchange ProxyShell vulnerability since at least October 2021 to gain initial access to systems in advance of follow-on operations, which include deploying ransomware. ACSC is also aware this APT group has used the same Microsoft Exchange vulnerability in Australia.

Find all CISA Cybersecurity Advisories here: Alerts | CISA