PRESS RELEASE | May 24, 2023

NSA and Partners Identify China State-Sponsored Cyber Actor Using Built-in Network Tools When Targeting U.S. Critical Infrastructure Sectors

The National Security Agency (NSA) and partners have identified indicators of compromise (IOCs) associated with a People's Republic of China (PRC) state-sponsored cyber actor using living off the land techniques to target networks across U.S. critical infrastructure.

"Cyber actors find it easier and more effective to use capabilities already built into critical infrastructure environments. A PRC state-sponsored actor is living off the land, using built-in network tools to evade our defenses and leaving no trace behind," said Rob Joyce, NSA Cybersecurity Director. "That makes it imperative

Skip to main content (Press Enter).

Rob Joyce, NSA Cybersecurity Director. "That makes it imperative for us to work together to find and remove the actor from our critical networks."

To assist network defenders to hunt and detect this type of PRC actor malicious activity on their systems, NSA is leading U.S. and Five Eyes partner agencies in publicly releasing the "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection" Cybersecurity Advisory (CSA) today. The partner agencies include:

- U.S. Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. Federal Bureau of Investigation (FBI)
- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- United Kingdom National Cyber Security Centre (NCSC-UK)

"For years, China has conducted operations worldwide to steal intellectual property and sensitive data from critical infrastructure organizations around the globe," said **Jen Easterly**, CISA Director. "Today's advisory, put out in conjunction with our US and international partners, reflects how China is using highly sophisticated means to target our nation's critical infrastructure. This joint advisory will give network defenders more insights into how to detect and mitigate this malicious activity. At the same time, we must recognize the agility and capability of PRC cyber actors, and continue to focus on strong cybersecurity practices like network segmentation and ongoing investments in promoting the resilience of critical functions under all conditions. As our nation's cyber defense agency, CISA stands ready to aid any organization affected and we encourage all organizations to visit our webpage for guidance and resources to make their networks more resilient."

"The FBI continues to warn against China engaging in malicious activity with the intent to target critical infrastructure

organizations and use identified techniques to mask their detection," said **Bryan Vorndran**, the FBI's Cyber Division Assistant Director**.** "We, along with our federal and international partners, will not allow the PRC to continue to use these unacceptable tactics. The FBI strives to share information with our private sector partners and the public to ensure they can better protect themselves from this targeted malicious activity."

"It is vital that operators of critical national infrastructure take action to prevent attackers hiding on their systems, as described in this joint advisory with our international partners," said **Paul Chichester**, NCSC Director of Operations**.** "We strongly encourage UK essential service providers to follow our guidance to help detect this malicious activity and prevent persistent compromise."

"The Canadian Centre for Cyber Security joins its international partners in sharing this newly identified threat and accompanying mitigation measures with critical infrastructure sectors," said **Sami Khoury**, Head of the Canadian Centre for Cyber Security. "The interconnected nature of our infrastructures and economies highlights the importance of working together with our allies to identify and share real-time threat information."

The CSA provides an overview of hunting guidance and associated best practices. It includes examples of the actor's commands and detection signatures. The authoring agencies also includes a summary of indicators of compromise (IOC) values, such as unique command-line strings, hashes, file paths, exploitation of CVE-2021-40539 and CVE-2021-27860 vulnerabilities, and file names commonly used by this actor.

As one of their primary tactics, techniques, and procedures (TTP) of living off the land, the PRC actor uses tools already installed or built into a target's system. This allows the actor to evade detection by blending in with normal Windows systems and network activities, avoiding endpoint detection and response

(EDR) products, and limiting the amount of activity that is captured in default logging configurations.

NSA recommends network defenders apply the detection and hunting guidance in the CSA, such as logging and monitoring of command line execution and WMI events, as well as ensuring log integrity by using a hardened centralized logging server, preferably on a segmented network.

Defenders should also monitor logs for Event ID 1102, which is generated when the audit log is cleared.

The behavioral indicators noted in the CSA can also be legitimate system administration commands that appear in benign activity. Defenders must evaluate matches to determine the significance, applying their knowledge of the system and baseline behavior.

Read the full report here.

Visit our full library for more cybersecurity information and technical guidance.

NSA Media Relations
MediaRelations@nsa.gov
443-634-0721

SHARE PRINT

Related Press Advisories

NSA, CISA, FBI Reveal Top CVEs Exploited by Chinese State-Sponsored Actors

NSA, CISA, and FBI Expose PRC State-Sponsored Exploitation of Network Providers, Devices

NSA, CISA, and FBI detail Chinese State-Sponsored Actions, Mitigations

Related Documents

CSA: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

cybersecurity mitigation endpoint security microsoft Windows tools Tactics Techniques and Procedures TTPs Endpoint Detection Malicious Actor TTPs Active Directory Network Security living off the land indicator of compromise IOC PRC guidance hunt