

New International Cyber Advisory Puts Threat Informed Control Validation in Focus

The October 8 advisory describes China-linked actors combining automated scanning, botnets, and hands-on exploitation to steal sensitive data

SCOTTSDALE, AZ, UNITED STATES, October 13, 2026 /EINPresswire.com/ --

A new joint cybersecurity advisory from the FBI, Cybersecurity and

Infrastructure Security Agency, National Security Agency, and international partners describes China-linked threat actors combining automated scanning with hands-on exploitation to obtain persistent access and steal sensitive data. The October 8, 2026, advisory gives security leaders a current basis for testing whether exposed services, identity controls, logging, and response procedures work against observed tactics rather than only against written requirements.

“

This advisory gives defenders concrete behavior to hunt for and concrete controls to validate, from exposed services and identity paths to logging, containment, and recovery.”

Michael Peters - Founder and CEO



Lazarus Alliance Proactive Cyber Security services
Logo

The authoring agencies said the activity was enabled by Integrity Technology Group, a China-based company with links to the Chinese government. They reported that the analysis draws on technical evidence from multiple FBI investigations. The advisory also cautions that commercial names for threat clusters do not necessarily map one-to-one to government attribution and that related actors may conduct activity outside the company's involvement.

According to the advisory, the actors used open-source scanning tools, a large-scale botnet, VPN infrastructure, known vulnerabilities, password attacks, and living-off-the-land techniques. The agencies identified targeting across U.S. critical infrastructure sectors and other organizations in North America, Southeast Asia, and Africa. They urged defenders to hunt for the published indicators and activity, strengthen controls, and update incident-response plans.

The practical lesson is broader than a single indicator list. Automated reconnaissance can repeatedly test the public attack surface, while an operator adapts after gaining a foothold. A control that existed during an annual review may be ineffective after a configuration change, an

exposed management interface, a stale account, a missed patch, or a logging gap. Organizations therefore need a repeatable way to compare current exposure and telemetry with current threat behavior.

A threat-informed review can start with internet-facing asset discovery, validation of unsupported or unpatched systems, authentication testing, and confirmation that unused services are disabled. Authorized vulnerability and penetration testing can then examine whether layered controls resist likely attack paths.

Detection validation should confirm that security teams can see scanning, unusual account use, credential attacks, lateral movement, and attempted access to high-value data. Incident exercises should test containment and evidence preservation as well as communications and recovery.

Lazarus Alliance supports risk assessment and management, vulnerability and penetration testing, cybersecurity audit and compliance, policies and governance, and Cybervisor® advisory services. Organizations using NIST SP 800-53, ISO/IEC 27001, or related frameworks can map the advisory's observed techniques to relevant control objectives, but they should validate implementation in the systems and identities that matter most to their operations.

"Threat intelligence becomes useful when it changes what an organization tests. This advisory gives defenders concrete behavior to hunt for and concrete controls to validate, from exposed services and identity paths to logging, containment, and recovery." - Michael Peters, CEO & Founder, Lazarus Alliance

ABOUT LAZARUS ALLIANCE

Lazarus Alliance is a veteran-owned global provider of Proactive Cybersecurity®, specializing in cybersecurity audit and compliance, risk assessment and management, privacy audit and compliance, vulnerability and penetration testing, and IT policies and governance. Founded in 2000, the firm helps organizations attain, maintain, and demonstrate information security and compliance excellence across complex regulatory environments.

Lazarus Alliance is an authorized CMMC Third-Party Assessment Organization (C3PAO), an A2LA-accredited FedRAMP Third-Party Assessment Organization (3PAO), and a PCI DSS Qualified Security Assessor (QSA). Headquartered in Scottsdale, Arizona, Lazarus Alliance serves organizations ranging from startups to multinational enterprises with cybersecurity, privacy, risk,



New International Cyber Advisory Puts Threat Informed Control Validation in Focus

The October 8 advisory describes China-linked actors combining **automated scanning, botnets, and hands-on exploitation** to steal sensitive data.

AUTOMATED SCANNING → **BOTNETS** → **HANDS-ON EXPLOITATION**

New International Cyber Advisory Puts Threat Informed Control Validation in Focus

The graphic features a world map with a red star over China, connected by red lines to server racks and a padlock icon. The text is in white and yellow, with a blue and orange background.

governance, and compliance expertise.

Michael Peters

Lazarus Alliance, Inc.

+17628224174 ext.

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/949317648>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.