THREAT BULLETINS

Joint Cybersecurity Advisory on Russian GRU Kubernetes Brute Force Campaign

TLP:WHITE

Jul 06, 2021

On July 1, 2021, the National Security Agency (**NSA**), Cybersecurity and Infrastructure Security Agency (**CISA**), Federal Bureau of Investigation (**FBI**), and the UK's National Cyber Security Centre (**NCSC**) released a Joint Cybersecurity Advisory regarding Russian General Staff Main Intelligence Directorate's (**GRU**) 85th Main Special Service Center (**GTsSS**), Unit 26165.

The joint advisory outlines Russia's malicious use of **Kubernetes** clusters cloaked by various virtual private network (VPN) providers and The Onion Router (TOR) to conduct widespread, distributed, and anonymized brute force access attempts against several government and private sector targets globally.

Kubernetes is an open-source system for orchestrating the deployment and management of software containers. This advisory is being shared to prevent a disruption of your network posture as these efforts are almost certainly still ongoing according to the Joint Cybersecurity Advisory.

The malicious cyber activity has previously been attributed to threat groups identified as **Fancy Bear**, **APT28, Strontium**, and a variety of others by the private sector. A significant amount of malicious activity was directed at organizations using Microsoft Office 365 cloud services in addition to targeting other service providers and on-premises email servers using a variety of different protocols.

This brute force capability allows the 85th GTsSS actors to access protected data, including email, and identify valid account credentials. Those credentials may then be used for a variety of purposes, including initial access, persistence, privilege escalation, and defense evasion. The actors have used identified account credentials in conjunction with exploiting publicly known vulnerabilities, such as exploiting Microsoft Exchange servers using CVE 2020-0688 and CVE 2020-17144, for remote code execution and further access to target networks. After gaining remote access, many well-known tactics, techniques, and procedures (TTPs) are combined to move laterally, evade defenses, and collect additional information within target networks.

For additional information including description of targets, known TTPs, detection and mitigation strategies, please see the joint cybersecurity advisory here.

Reference(s)	Defense, NSA, Health Industry Cybersecurity Practices, wikipedia, The Register, Bleeping Computer, Threat Post
Report Source(s)	CISA, FBI, NCSC, NSA

Recommendations

Network managers should adopt and expand usage of multi-factor authentication to help counter the effectiveness of this capability. Additional mitigations to ensure strong access controls include time-out and lock-out features, the mandatory use of strong passwords, implementation of a Zero Trust security model that uses additional

attributes when determining access, and analytics to detect anomalous accesses. Additionally, organizations can consider denying all inbound activity from known anonymization services, such as commercial virtual private networks (VPNs) and The Onion Router (TOR), where such access is not associated with typical use.

Please see the following for additional recommendations:

- Use multi-factor authentication with strong factors and require regular reauthentication.

- Strong authentication factors are not guessable, so they would not be guessed during brute force attempts.

- Enable time-out and lock-out features whenever password authentication is needed.

- Time-out features should increase in duration with additional failed login attempts.
- Lock-out features should temporarily disable accounts after many consecutive failed attempts. This can force slower brute force attempts, making them infeasible.

- Some services can check passwords against common password dictionaries when users change passwords, denying many poor password choices before they are set.

- This makes brute-force password guessing far more difficult.

- For protocols that support human interaction, utilize captchas to hinder automated access attempts.
- Change all default credentials and disable protocols that use weak authentication (e.g., clear-text passwords, or outdated and vulnerable authentication or encryption protocols) or do not support multi-factor authentication.

- Always configure access controls on cloud resources carefully to ensure that only well maintained and well-authenticated accounts have access.

- Employ appropriate network segmentation and restrictions to limit access and utilize additional attributes (such as device information, environment, access path) when making access decisions, with the desired state being a Zero Trust security model.
- Use automated tools to audit access logs for security concerns and identify anomalous access requests.

Sources
NSA-CISA-NCSC-FBI Joint Cybersecurity Advisory on Russian GRU Brute Force Campaign

NSA, Partners Release Cybersecurity Advisory on Brute Force Global Cyber Campaign

Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Publication

Kubernetes
TheRegister - Russia Gives Enterprises, Cloud Platforms a Free Brute-Force Security Test Using Kubernetes Clusters
BleepingComputer - NSA: Russian GRU Hackers Use Kubernetes To Run Brute Force Attacks
ThreatPost - Widespread Brute-Force Attacks Tied to Russia's APT28

Alert ID deb5f062

View Alert

Tags Joint Cybersecurity Advisory, NSA, NCSC, CISA, FBI

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

For Questions or Comments Please email us at toc@h-isac.org


For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.