SECURITY ADVISORY

CYBER STASH

September, 2024

Neutralizing Russian Military Cyber Threats

Context

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) have identified cyber actors associated with the Russian General Staff Main Intelligence Directorate (GRU), specifically the 161st Specialist Training Center (Unit 29155), as responsible for sophisticated cyber operations targeting global entities. Since at least 2020, Unit 29155 has engaged in activities aimed at espionage, sabotage, and inflicting reputational damage. Notably, these actors have employed the destructive WhisperGate malware against several Ukrainian organizations starting January 13, 2022. It is important to distinguish Unit 29155 from other GRU cyber units such as Unit 26165 and Unit 74455, as their tactics and targets differ significantly.

Mitigation

Defending against the Russian General Staff Main Intelligence Directorate (GRU) necessitates a proactive approach that includes reducing exposure to potential attacks, enhancing adversary detection and response capabilities, and mitigating vulnerabilities effectively.

Patch System and Application Vulnerabilities: Regularly patch system and application vulnerabilities.

Monitor and Update EDR: Stay informed about EDR bypass techniques and regularly update your EDR systems. Keep your EDR engine independent from your EPP (Endpoint Protection Platform) to reduce the risk of both systems being evaded if one is compromised.

Block High-Risk Sources: Use geo-blocking and filtering to restrict access from high-risk countries, ASNs, and TLDs to reduce exposure to potential attacks. See next pages for IOCs to block.

Secure and Test Backups: Implement regular, automated backups with secure storage and periodically test restoration processes to ensure data integrity and availability.

Enforce Multi-Factor Authentication for Exposed Services: Enable phishing-resistant multifactor authentication (MFA) for all externally facing account services, particularly for webmail, virtual private networks (VPNs), and accounts accessing critical systems.

Technical Details

For technical details, please refer to the following references:

CISA Advisory AA22-057A
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

MITRE ATT&CK S0689
https://attack.mitre.org/software/S0689/

Neutralizing Russian Military Cyber Threats
To enhance security, it is recommended that organizations take action to block the following adversary infrastructures. As adversaries are likely to frequently change their IP addresses, it is recommended to enforce blocking measures using GEO-IP and ASN (Autonomous System Number) filtering where possible. By focusing on GEO-IP and ASNs, you can address broader patterns of malicious infrastructure rather than individual IPs. Adversaries are less likely to change the underlying infrastructure they use for attacks, making this approach more effective in preventing access and mitigating threats.

Country	ASN	IP Addresses	Organization
United Kingdom	25369	5.226.139.[66]	Hydra Communications Ltd
Russia	206728	45.141.87.[11], 194.26.29.[84], 194.26.29.[95], 194.26.29.[98], 194.26.29.[251]	Media Land LLC
	34300	62.173.140.[223]	Internet-Cosmos LLC
Germany	14061	46.101.242.[222]	DigitalOcean, LLC
Netherlands	208046	79.124.8.[66]	ColocationX Ltd.
Latvia	1257	90.131.156.[107]	Tele2 Sverige AB
China	9808	112.51.253.[153]	China Mobile Communications Group Co., Ltd.
	4837	112.132.218.[45]	CHINA UNICOM China169 Backbone
United States	174	154.21.20.[82]	Cogent Communications
Switzerland	51852	179.43.133.[202], 179.43.142.[42], 179.43.162.[55], 179.43.175.[38], 179.43.175.[108], 179.43.176.[60], 179.43.187.[47], 179.43.189.[218]	Private Layer INC
Denmark	9009	185.245.84.[227]	M247 Europe SRL
Slovakia	9009	185.245.85.[251]	M247 Europe SRL

WARNING

Before blocking these countries and ASNs, be aware that legitimate services may also be hosted on these infrastructures. Ensure thorough analysis to avoid disrupting legitimate operations.

References

IOCs:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

Public Intelligence:

CISA Advisory AA22-057A
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

MAR-10375867-1.v1 – HermeticWiper
- https://www.cisa.gov/news-events/analysis-reports/ar22-115a

MAR-10376640-1.v1 – IsaacWiper and HermeticWizard
- https://www.cisa.gov/news-events/analysis-reports/ar22-115b

MAR-10376640-2.v1 – CaddyWiper
- https://www.cisa.gov/news-events/analysis-reports/ar22-115c

MITRE ATT&CK S0689
- https://attack.mitre.org/software/S0689/