ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness of cyberattacks against critical infrastructure warned by CISA and FBI.

Summary

Recent intelligence indicates an escalating threat to critical infrastructure worldwide, primarily attributed to state-sponsored cyber actors from Russia and China.

Russian cyber operations, particularly those linked to the GRU’s Unit 29155, have been active since early 2020, targeting sectors such as government, energy, and healthcare. Notable incidents include the deployment of WhisperGate malware against Ukrainian organizations, aiming for disruption and reputational damage.

Similarly, Chinese cyber activities have gained attention with the disruption of the "Flax Typhoon" hacking group, responsible for establishing a botnet that has infected hundreds of thousands of devices. This group has targeted critical infrastructure across the U.S., Canada, and Europe, indicating a significant threat to operational continuity and data integrity.

In light of these developments, organizations are urged to adopt proactive measures to strengthen their cybersecurity posture.

Russian Cyber Operations

The FBI, CISA, NSA have identified cyber actors affiliated with the Russian GRU's Unit 29155 as responsible for numerous cyberattacks since 2020. This group employs a variety of tactics, focusing on espionage, sabotage, and reputational damage.

As early as January 2022, Unit 29155 began deploying WhisperGate malware against Ukrainian organizations, indicating an aggressive approach to cyber warfare. This malware is designed for destructive purposes, aimed at disrupting the operations of targeted entities.

Their operations have primarily focused on critical infrastructure sectors, including government services, financial institutions, energy, transportation, and healthcare. The FBI noted over 14,000 scanning incidents across at least 26 NATO members and various EU countries, demonstrating the widespread nature of their cyber reconnaissance efforts.

The advisory highlights ongoing campaigns targeting organizations providing aid to Ukraine, with tactics including website defacements and data leaks to cause reputational harm and operational disruptions.

Chinese Botnet Activities

The FBI recently disrupted the "Flax Typhoon" hacking group, which is alleged to operate on behalf of the Chinese government. This group compromised a vast network of devices worldwide, targeting critical infrastructure within the U.S. and beyond.

Flax Typhoon established a botnet by installing malicious software on various IoT devices, including routers, cameras, and video recorders. This botnet has reportedly infected over 250,000 devices globally, allowing the group to conduct extensive reconnaissance and data theft operations.

Targets included government agencies, telecommunications providers, universities, and NGOs. The FBI emphasized that these cyber actions caused significant operational disruption, forcing victims to allocate resources to mitigate the effects of the malware.

The Integrity Technology Group, which the FBI claims is behind Flax Typhoon, has been accused of posing as an IT firm while gathering intelligence for Chinese security agencies. China has denied these allegations, asserting that it takes action against cyberattacks.

The responses to both Russian and Chinese cyber threats underscore the importance of international collaboration among cybersecurity agencies. The recent joint advisory from the FBI, CISA, and allied nations emphasizes the need for a collective approach to addressing these advanced threats.

Recommendations

Recommendation #1: Stay up to date

Stay informed about the latest cybersecurity threats and vulnerabilities by regularly monitoring advisories and updates from trusted sources such as CISA, NSA, and FBI. In the event of a cyberattack or suspicious activity, inform them.

Recommendation #2: Routine System Updates

Consistently update and patch systems to eliminate known vulnerabilities. For instance, the Russian GRU actors exploited vulnerabilities like CVE-2021-33044 and CVE-2022-26134 to gain initial access to systems. Regular updates are crucial to protect against similar exploits.

Recommendation #3: Enforce MFA

Implement robust MFA for all externally facing services, especially those granting access to critical systems.

Recommendation #4: Network Segmentation

Employ network segmentation to isolate critical systems and prevent the lateral movement of adversaries within the network.

Recommendation #5:Proactive Monitoring

Establish vigilant monitoring for unusual scanning activities indicative of reconnaissance efforts by cyber adversaries.

Recommendation #6: Prepare for the Worst

ORNA **strongly recommends** that organizations ensure that all critical systems are backed up appropriately and that incident response plans are rehearsed regularly so that all participants understand their role.

References

1. CISA: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

2. Cyberscoop: https://cyberscoop.com/fbi-operation-china-botnet-flax-typhoon/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team