Cybersecurity

Cyber Threat Intelligence and Incident Response Report

Cyber threat intelligence is information that is collected and evaluated by an organization to better understand the intents, capabilities, and TTPs of the malicious actors that pose threats.

Cyber threat intelligence helps reduce the risk of repeated breaches by allowing for risk mitigation strategies.

Incident Name	Black Basta
Report Author	CISA
Report Date	Nov 8 2024

1. What was the indicator of attack?

Spikes in file encryption activity and suspicious processes

2. What was the adversarial motivation (purpose of attack)?

Financial gain

3. What were the adversary's actions and tactics?

Phishing, spear phishing voice, and exploit public-facing application

Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table.

Reconnaissance	Scanning for OSINT, RDP, VPN, or SMB services
Weaponization	Qakbot or SocGholish as an initial loader Weaponized office docs with malicious links embedded by scripts
Delivery	Phishing, exploiting public-facing systems, malvertising
Exploitation	Office files containing malware execute payloads Brute force or credential stuffing attacks Abusing LOLBins like Powershell or run scripts
Installation	Drops a RAT, installs persistence mechanisms, moves laterally with mimikats or abusing LSASS
Command and Control	Encypted traffic over http/https or DNS tunneling Qakbot's C2 infrastructure
Actions on Objectives	Data exfiltration using tools like Rclone, Mega, or FileZilla Encrypts files in a ransomware payload

4. What are your recommended mitigation strategies?

General hardening, User awareness, Endpoint and network monitoring, access controls, incident response teams.

5. List your third-party references.

CISA and MITRE ATT&CK