THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Hunters

Threat Actor

Ransomware

CATEGORY

Ransomware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Data Breaches
- Financial Losses
- Disruptions and Downtime
- Reputational Damage

Description

Hunters

In 2024, Hunters International, a RaaS group that emerged in late 2023, has conducted ransomware attacks in nearly 20 countries. Notably, their code shows significant overlap with the Hive strain, disrupted by law enforcement earlier in 2023, suggesting a possible evolution or offshoot of the Hive group. Employing a dual strategy, they encrypt critical data on compromised systems and exfiltrate it for additional extortion by threatening to leak the stolen data on the dark web. This tactic pressures victims into paying for decryption and to prevent exposure of sensitive information. While the origins of Hunters International are unclear, some speculate a Russian connection based on domain registration patterns, though inconsistencies in their communication emails cast doubt on this theory. This group poses a significant threat to various sectors, evidenced by their targeting of healthcare institutions and major corporations.

Indicator of compromise

SHA-256

94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af

24de8de24001bc358c58aa946a28c545aaf9657b66bd5383c2d5a341c5d3c355

Remediation

1. Update and Patch Systems: Regularly apply security patches and updates to all software and operating systems.
2. Backup Data: Maintain frequent, secure backups of critical data and store them offline or in a separate network.
3. Network Segmentation: Implement network segmentation to limit the spread of ransomware within the organization.
4. User Training: Conduct regular cybersecurity awareness training for employees to recognize phishing attempts and other attack vectors.
5. Access Controls: Enforce strict access controls and least privilege principles to minimize unauthorized access.
6. Incident Response Plan: Develop and regularly update an incident response plan specific to ransomware attacks.
7. Multi-Factor Authentication (MFA): Implement MFA for all user accounts to enhance security.
8. Regular Audits: Perform regular security audits and vulnerability assessments to identify and mitigate potential risks.
9. Monitor and Detect: Use intrusion detection and prevention systems (IDPS) to monitor network traffic for suspicious activities.
10. Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Secure your byte world

☎ +1 (832) 271 2738

✉ info@threatcure.net

🌐 https://threatcure.net/