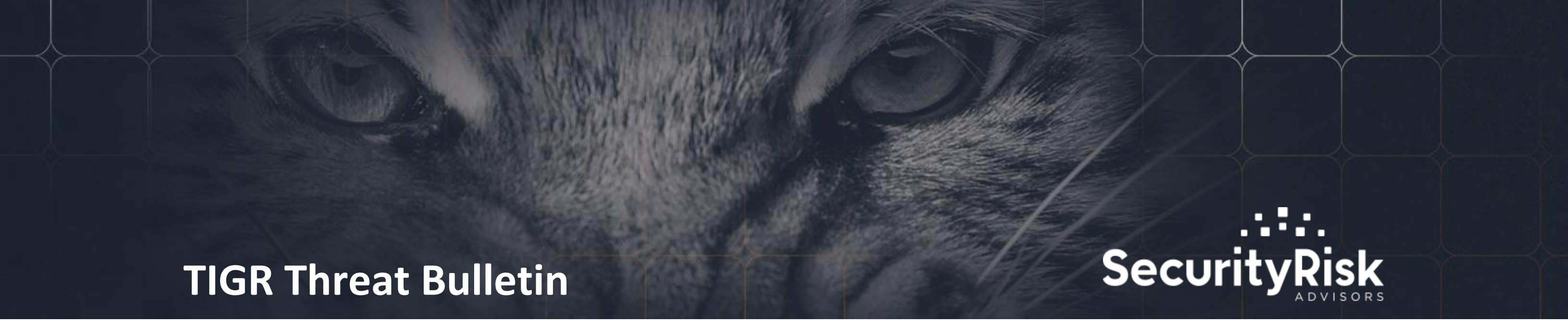

TIGR Threat Bulletin

SecurityRisk ADVISORS

New ‘Fog’ Ransomware Group Identified

June 7, 2024

Executive Summary

Artic Wolf Labs identified a new ransomware variant cited as ‘Fog.’ Fog ransomware appears to be used against US-based educational institutions and occasionally US-based recreation companies. Ransomware groups deploying Fog appear to gain access to environments via compromised virtual private network (VPN) credentials. Following compromised credentials, hacking tools are used to engage in reconnaissance and lateral movement to aid ransomware deployment. Currently, threat actor activity linked to Fog ransomware is not associated with data leak sites and data exfiltration.

Impact

Fog ransomware poses a risk to organizations with insufficient offsite backups. Most organizations impacted by the ransomware fall into the education or recreation sectors. Affected companies could lose business-critical data and be forced to stop operations or pay a ransom. Threat actors utilizing Fog can cause direct financial losses, loss of revenue, reputational damage, or regulatory penalties. Organizations without offsite backups might still be affected, as the threat actor has been observed deleting shadow volume snapshots and Veem backups to inhibit recovery. Currently, the threat actor does not appear to be disclosing or exfiltrating sensitive information.

Safeguards/Recommendations

Educational and recreation organizations should review and complete, where possible, the following:

- Monitor for indicators of compromise & complete ad-hoc hunts based on the techniques published by Artic Fox.
- Actively monitor for abnormal VPN sign-ins, unauthorized configuration changes, such as the removal or tampering with EDR tools, and the use of network scanners or enumeration of network shares.
- In addition to active monitoring, SRA will be conducting ad-hoc IOC sweeps & threat hunts for SRA’s educational and recreation CSOC / XDR customers in all logs available to CSOC:
    - The presence of the 12 IPv4 and SHA1 indicators provided by Artic Fox
    - The presence of any of the 10 file names and 6 tools used by the adversaries

References

- https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat/