

More Information

Capabilities

Framework and resources:

<https://arkime.com/>

Working with the API:

<https://arkime.com/api>

Plugins:

<https://arkime.com/settings#plugins>

Elasticsearch over TLS

<https://arkime.com/esssl>

Related Information

Articles and presentations

<https://arkime.com/articles>

List of subjects in the area

- Phishing
- C2
- Data exfiltration
- Lateral movement
- Host/Environment discovery

<https://github.com/jstrosch/malware-samples>

