How’s that for a malicious Linkc, new group launches DLS

cyjax.com/resources/blog/new-extortion-ransomware-group-linkc-emerges-what-you-need-to-know/

21 February 2025

Introduction

2024 saw data-leak sites (DLSs) for 72 extortion groups materialise. As of February 2025, Cyjax has identified DLSs for five new groups, as noted in recent blogs on extortion groups Kraken, Morpheus, GD LockerSec, and Babuk2. The fifth one to emerge goes by the name Linkc. Read on to find out what Cyjax knows so far about this new entrant into the data leak extortion scene.

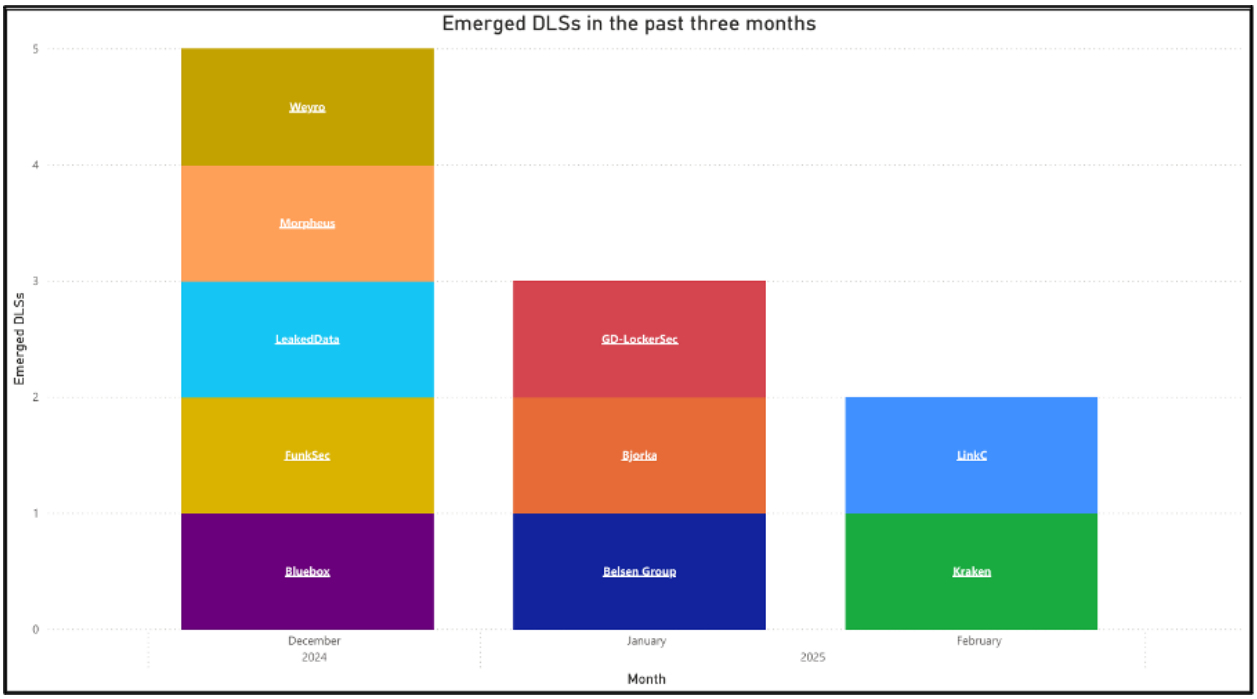

Figure 1 –New extortion groups Cyjax has observed over the last 3 months.

Key takeaways

- On 29 January 2025, Linkc claimed a breach of AI and cloud organisation H2O.ai on its DLS, a Tor (onion) hosted website.
- The group claims to have access to a large amount of the organisation’s private information and has provided alleged data samples as evidence. H2O.ai has not acknowledged this purported attack.
- A second, private onion site likely belonging to the group has also emerged. This site requires users to log in and potentially holds additional information in comparison to what is found on the public DLS.

- Threat actors have not discussed Linkc or shared links to the group's DLS on popular cybercrime forums.

Context

Extortion groups commonly use DLSs to further extort victims, typically proceeding in multiple stages. The first threat is that the victim's name and news of a successful attack against it will be published on the extortion group's website. Should this fail to motivate a victim to pay a ransom, the group's next step is typically to provide proof of the successful theft of its data, such as screenshots of internal file trees, samples of employee or customer PII, or other sensitive documents. The group may add a countdown at this stage, noting that should the victim fail to pay by the conclusion, it will make available to DLS visitors all stolen data, either for free or at cost.

Victimology

As of 20 February 2025, only one victim is listed on the Linkc DLS, namely the US-based AI developer and cloud service provider H2O.ai. The organisation advertises its services for use cases in the finance, government, health, insurance, manufacturing, marketing, retail, and telecommunication sectors. H2O.ai has not released any statement regarding this supposed attack. The post was listed on 29 January 2025.

Linkc claims to have discovered:

- *"unanonymized user datasets intended for AI training".*
- *"Full source code of programs from the Git repository, including code for driverless systems, GPT models, and others".*
- *"A substantial amount of internal information, including contracts, customer personal data, project costs, and project documentation".*
- *"Backup copies of employee email accounts containing customer correspondence*".

Linkc has provided screenshots of databases, legal documents, and a link to a CSV of information purportedly stolen from H2O.ai within the listing on its DLS. This can be seen in ***Figure 2***. Cyjax has examined these documents and found references to other organisations. There is currently no way of accessing the entire collection of data Linkc claims to have stolen. Unlike many other DLSs, there is no countdown indicating when the data will be released.

Figure 2 – A section of the Linkc DLS listing for H2O.ai.

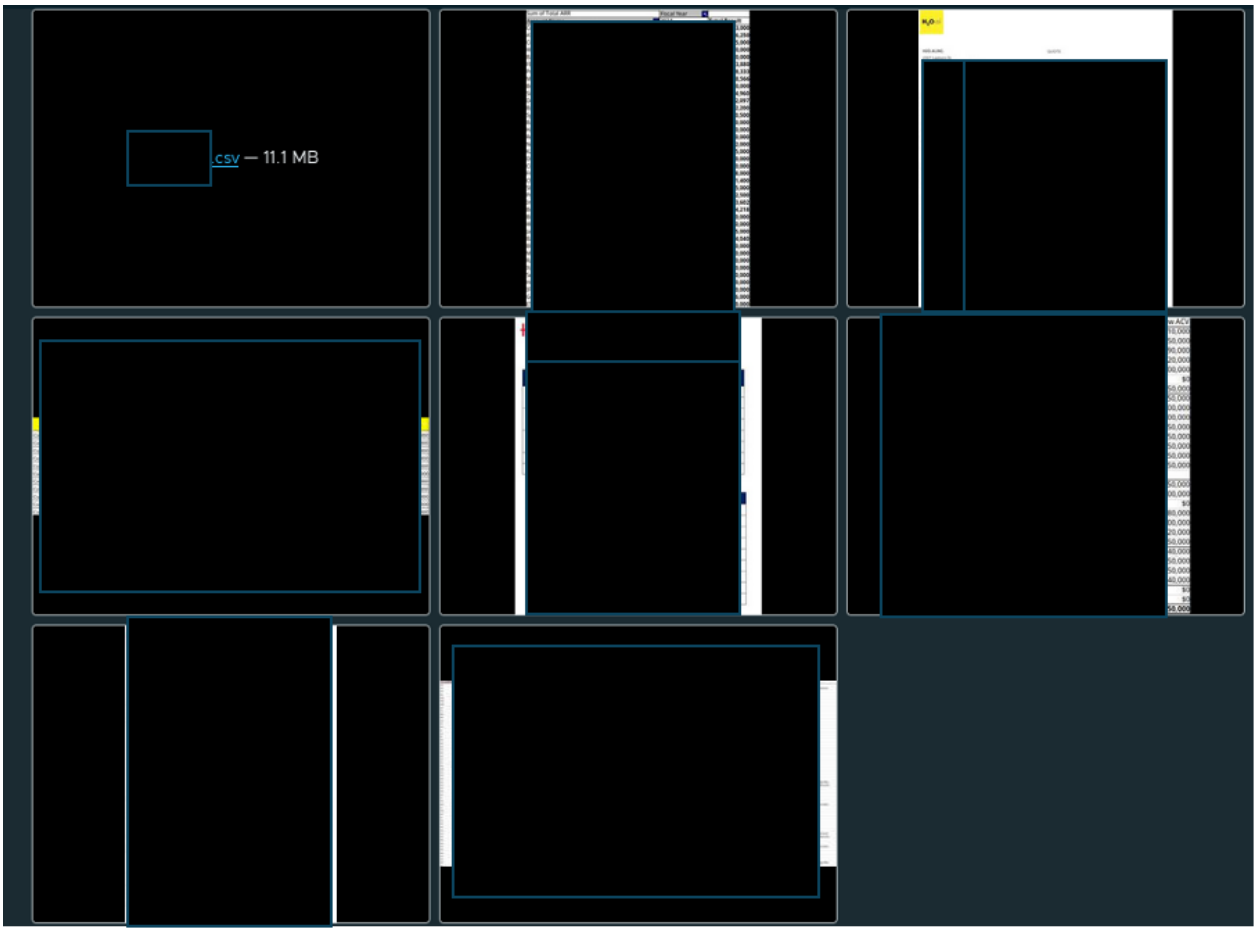

Figure 3 – The lower half of the H2O.ai listing.

The Linkc DLS

Linkc's DLS is well made, quick to load, and has suffered no down time in the time period Cyjax has attempted to access the site. In the upper left-hand corner of the site there is the title "*Linkc Pub*", which is likely short for 'public'. As such, this possibly implies the existence of a private DLS. A pop-up menu to the left of the site only features a single option titled "*Articles*". Clicking this takes the visitor to the main page of the DLS which lists the victim. It is likely that additional victims are intended to be displayed in a grid of cards, where each one displays the name, date of listing, logo, and a brief description of the organisations. As of 20 February 2025, only one card exists. However, a search feature is found above this victim grid which implies that the group intends to have a large collection of future victims.

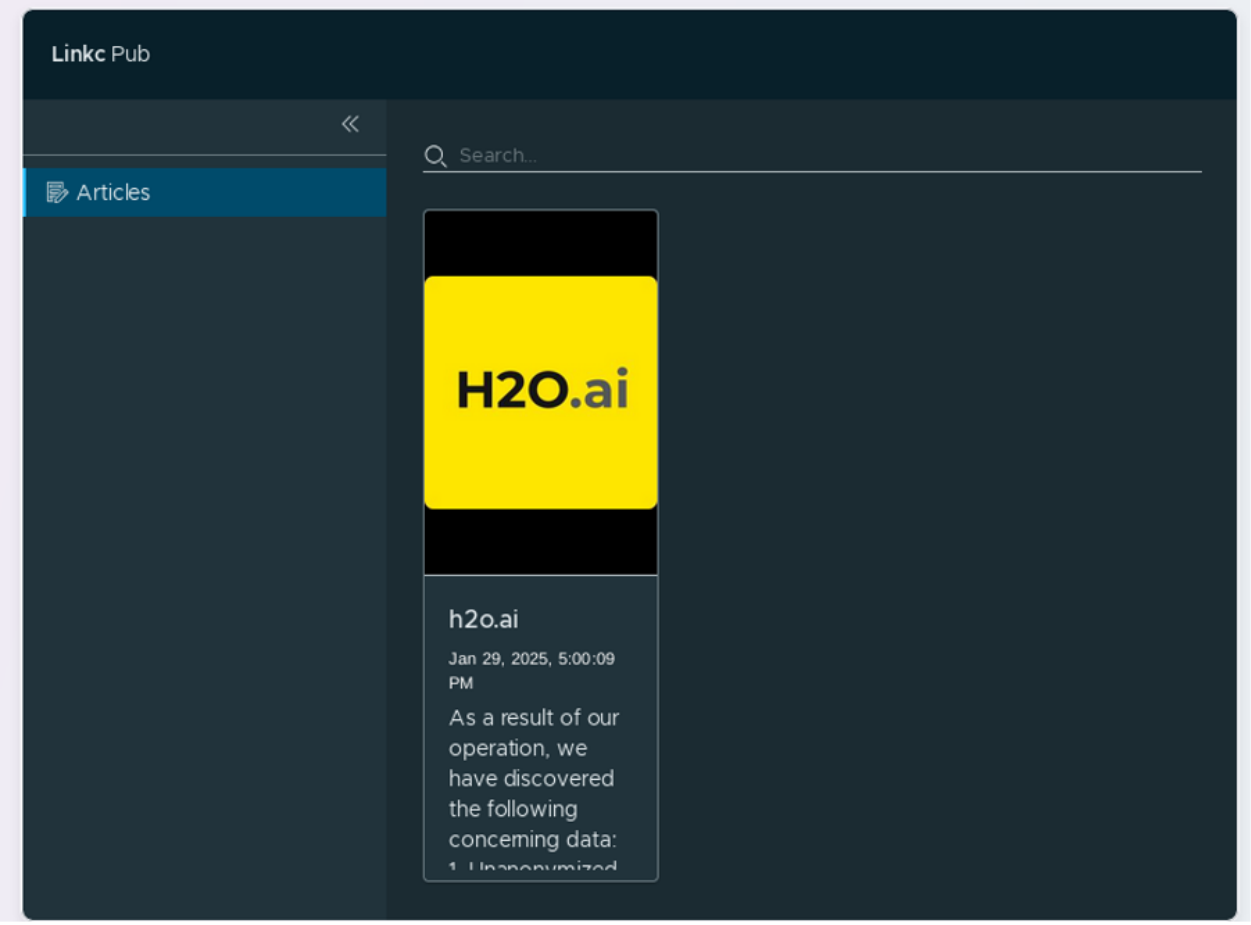

Figure 4 – The view of the Linkc DLS homepage.

File names and references in the sites HTML indicate the DLS was created with the use of HTML, CSS, JavaScript, and Angular.

A second onion site has been tied to the group. When visiting, users are asked to "*Enter Secret*" before being allowed to log in. Login details for this are not publicly available and it is likely that Linkc provides them directly to victims. The site's HTML features the same Angular, JavaScript and CSS file names as Linkc's DLS, implying that the same developers of the Linkc DLS are behind the creation of this onion site.

Figure 5 – View of the second onion site Linkc hosts

```
<app-root ng-version="18.2.4">
  <router-outlet></router-outlet>
  <app-public-shell _nghost-ng-c2363653013="">…</
  app-public-shell>
  <!---->
</app-root>
<script src="polyfills-SCHOHYNV.js" type="module"></
script>
<script src="main-6UGWMGZ6.js" type="module"></
script>
```

Figure 6 – Sample of HTML containing script SRCs and 'ng-host' files found on both sites.

Other locations

Cyjax has not identified any accounts on popular cybercriminal forums which operate under the name of Linkc. Additionally, there has been no threat actor discussion or promotion of Linkc and the group's DLS onion site address has not been shared.

Threat Assessment

As of February 2025, there is little available information regarding the Linkc group. Its only alleged victim has not acknowledged any attacks, Linkc has made no announcement on how it supposedly obtained the data, and other threat actors have not discussed the group's claims. However, the group does appear to have access to at least some sensitive information and may possess the skills to perform further ransomware attacks. The ransomware landscape is developing and evolving, meaning Linkc is likely to claim further attacks and victims in the future.

To access our full intelligence repository containing detailed profiles like this one, covering extortion groups, advanced persistence threat groups (APTs), data brokers, hacktivists, initial access brokers, and more, click here to take a test drive of Cymon.

Receive our latest cyber intelligence insights delivered directly to your inbox

Simply complete the form to subscribe to our newsletter, ensuring you stay informed about the latest cyber intelligence insights and news.