An elephant in Kairos: data-leak site emerges for new extortion group - CYJAX

By Roman Faithfull

Published: 2024-11-14 · Archived: 2026-04-05 19:09:25 UTC

Table of contents

It is nearing 2025, and data-leak sites (DLSs) for extortion groups continue to emerge. November 2024 continues this trend, with Cyjax observing the thirteenth most recent materialisation of a DLS for an extortion group calling itself “Kairos”. At the time of writing, Kairos has claimed attacks against six victims, two of which have acknowledged significant data breaches in 2024. However, it is unclear whether these are related.

Read on to find out what Cyjax knows so far about this new player in the extortion group ecosystem.

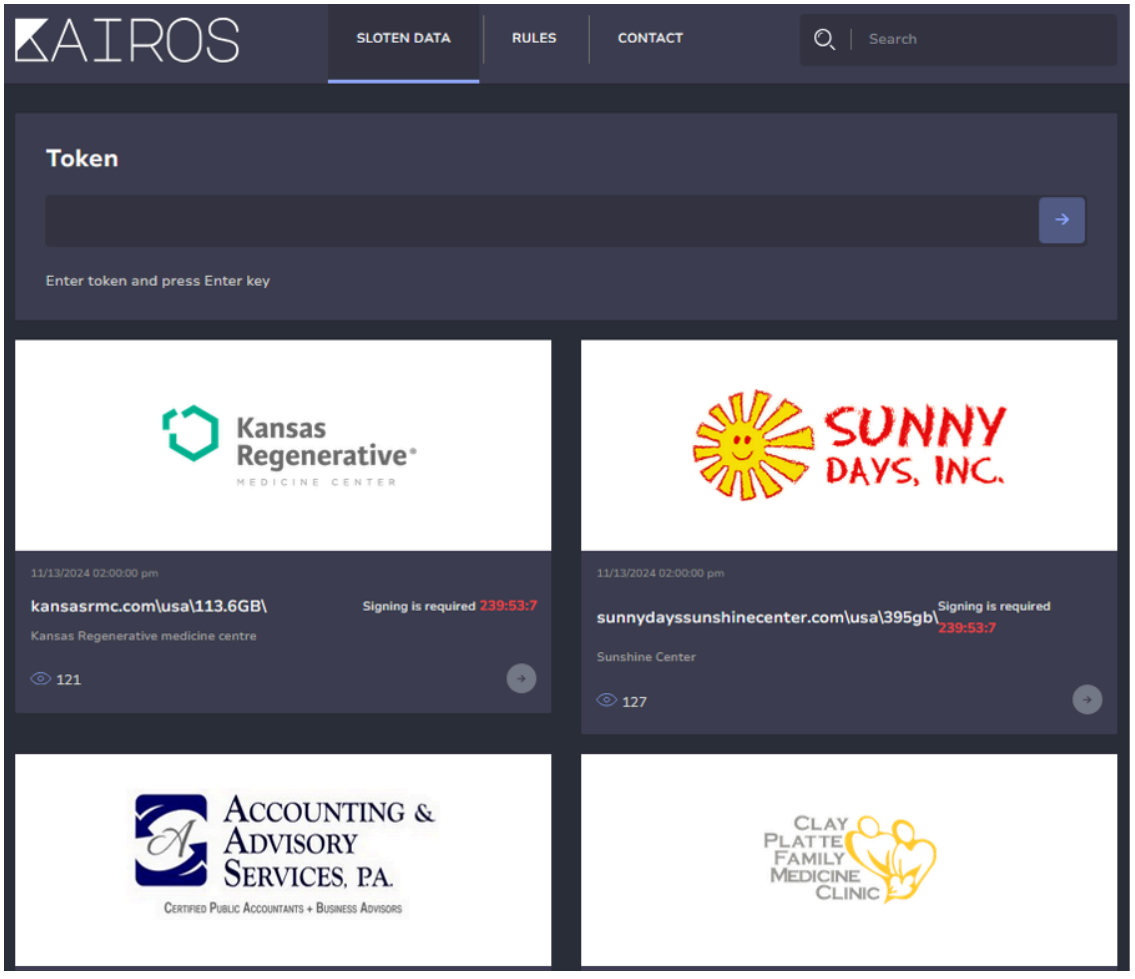

Figure 1. Kairos DLS landing page, displaying a list of organisations the group claims to have attacked.

Context

Extortion groups commonly use DLS 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.

History and Victimology

The Kairos DLS emerged on or around 13 November 2024 and has so far claimed attacks against six organisations, with a focus on the US and the healthcare sector. These are:

- US-based The Physical Medicine and Rehabilitation Center.
- Taiwan-based Formosa Certified Public Accountants.
- US-based Clay Platte Family Medicine Clinic.
- US-based Ask Your Accountant Accounting & Advisory Services.
- US-based healthcare services provider Sunshine Center.
- US-based Kansas Regenerative Medicine Center.

None of these organisations have released public statements since being named on Kairos' DLS. However, it is notable that Clay Platte Family Medicine and The Physical Medicine and Rehabilitation Center experienced significant data breaches in 2024 which occurred, in June and July, respectively. The organisations did not indicate the identity of their attackers in these public statements. Should Kairos' claims of compromise be legitimate, it is unclear whether the attacks occurred independently, or if they stemmed from any information exposed during these Summer 2024 attacks, or whether they are one and the same.

It is notable that Kairos targeted a Taiwan-based organisation. Cyjax recently observed a large increase in advertisements for initial access to Taiwanese organisations on cybercriminal forums, the details of which can be found in our whitepaper on the 2024 Q3 initial access broker (IAB) market.

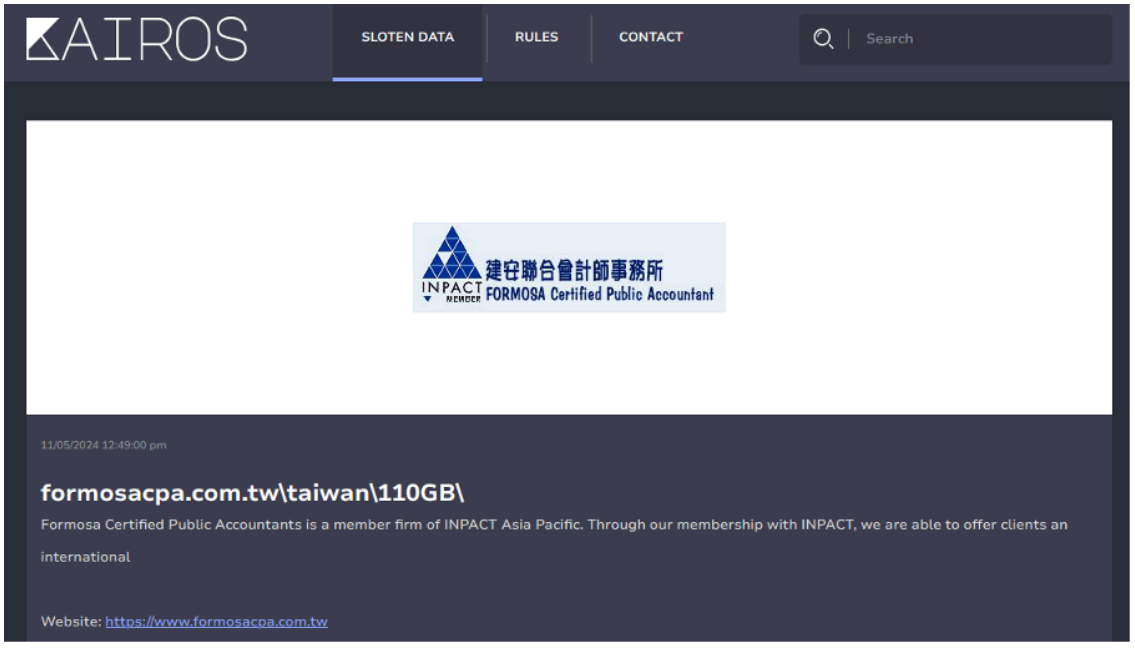

Figure 2. Kairos victim post for Formosa Certified Public Accountants

It is realistically possible that Kairos has successfully attacked other organisations that paid in the first instance of a ransom being demanded. As such, they were not named on the site and are not known to the public. However, Cyjax cannot confirm this.

The Kairos DLS

The group's TOR-hosted DLS consists of three main pages:

Landing page

The site's landing page hosts a list of organisations which the group claims to have attacked. This includes a description of each victim, its logo, the likely date on which it was named on the site, the amount of data allegedly stolen, and a countdown for when "Signing is required". This likely refers to the time after which the group will publish stolen data in full if the victim does not pay. Clicking on the victim's logo directs to a specific page for each, providing a more detailed description of the organisation and sample images of allegedly stolen data. This data includes personally identifiable information (PII), as well as legal, fiscal, and medical documents.

There is an interesting discrepancy between the dates displayed on the site. On the landing page, each victim post displays 13 November 2024, seemingly indicating the date on which these victims were named on the DLS. However, navigating to the individual victim pages on the DLS gives earlier dates. Of these, Sunny Days, Inc. is listed with the earliest of 16 October 2024. Other victim pages list 5 and 11 November 2024. As such, this may refer to the date on which Kairos first compromised each victim.

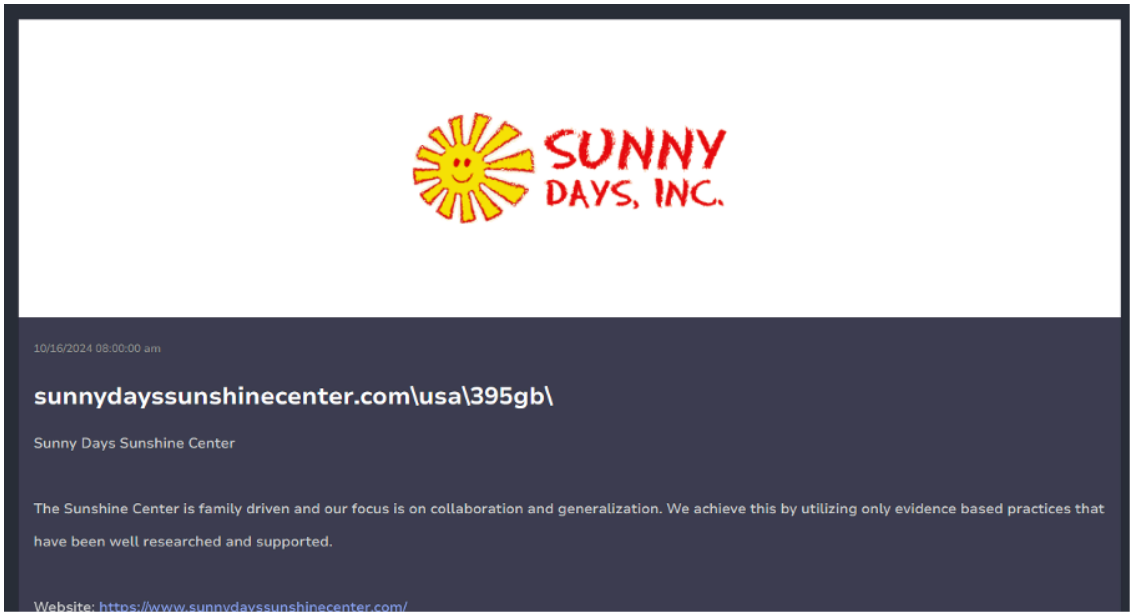

Figure 3. Kairos victim post for Sunny Days, Inc listing the 16 October 2024 date.

Rules page

The DLS hosts a "Rules" page, which provides insights into the group's operation and motivation. Kairos is apparently purely financially motivated, demanding payment in exchange for the safe return of stolen files and to not leak them publicly. By way of proof of exfiltration, the group offers to send the victim five stolen files of their choosing from a list of those that do not contain "critical" information.

The rules stipulate that victims must make payment via Bitcoin and have 7 days to comply. Though the specific monetary amounts the group demands are not public, it claims that the price is dependent on the victims' "income, expenses, documents, and reports" and is non-negotiable. However, a 20% discount is offered to those who make payment within 5 days of the initial request. Kairos promises to delete stolen files within 24 hours of receiving a ransom payment. It also claims to provide paying victims with a "security report with recommendations".

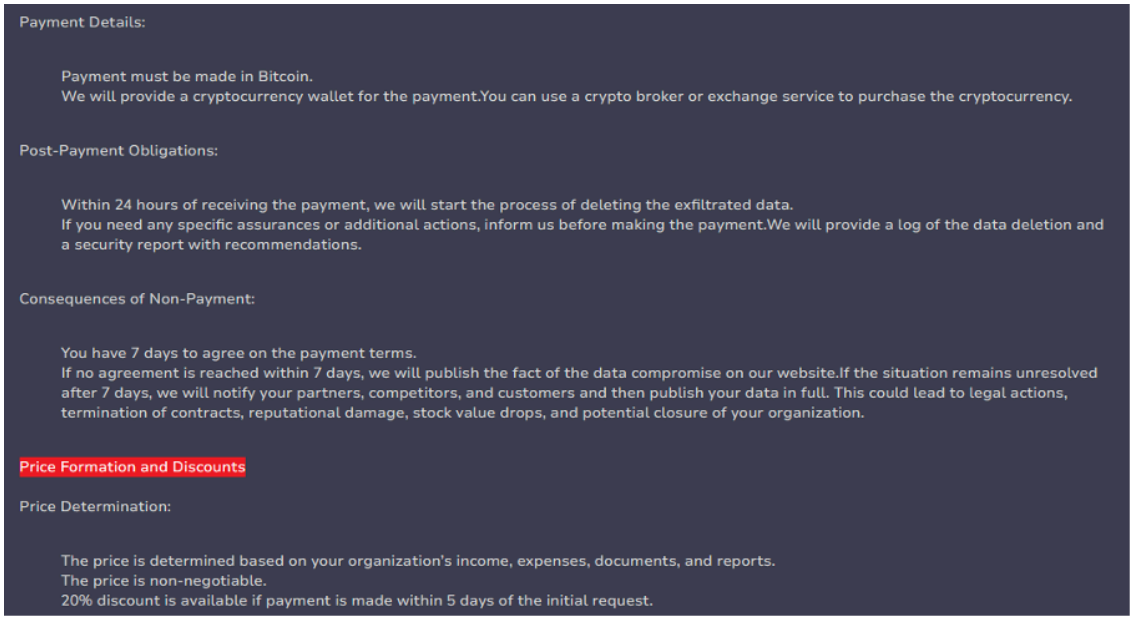

Figure 3. Kairos Rules page detailing ransom payment and file deletion

Token page

Thirdly, the site has a page with a Token input box. Presumably, victims receive a unique token in the Kairos ransom note, which they can use to navigate to a non-public-facing part of the DLS and initiate communication with the group.

Data-leak only

The rules page notes the group provides “Guidelines for Responding to Data Exfiltration and Extortion Demands Understanding the Situation”. Given the lack of reference to encryption in the group’s rules, Cyjax does not believe Kairos operates as a ransomware operation at this time. The group writes that it has conducted a “thorough investigation” of its victims’ networks and downloaded all “confidential, private, proprietary, legal, financial, and compromising information” belonging to its customers and employees and demands payment for the “secure deletion” of this. The group threatens that should victims not pay, it will make publicly available their stolen data to visitors of the DLS.

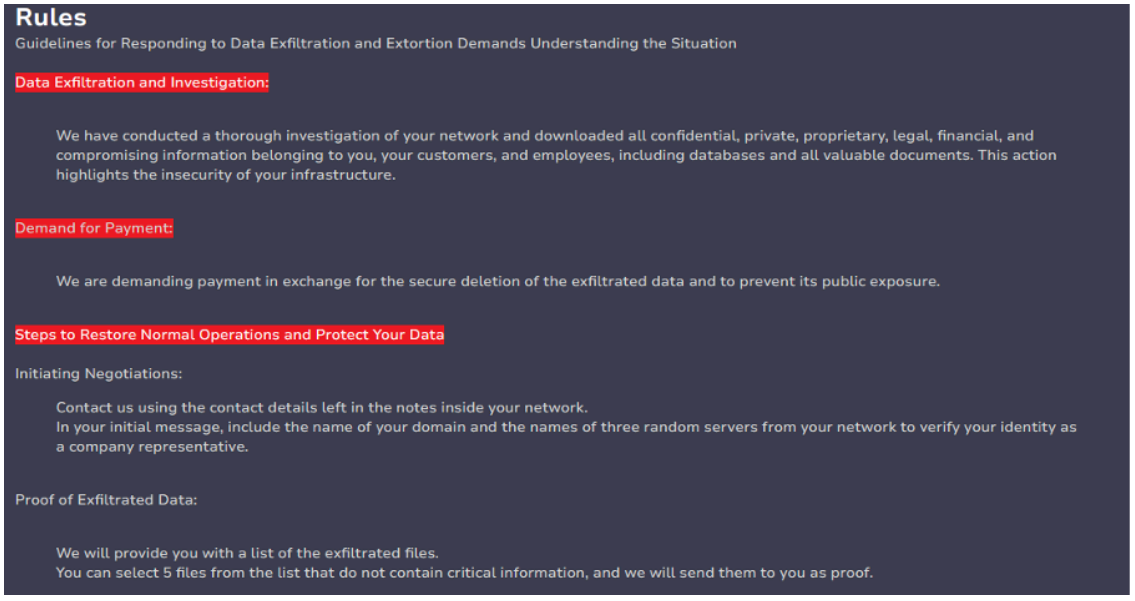

Figure 4. Kairos Rules page detailing “Guidelines for Responding to Data Exfiltration and Extortion Demands Understanding the Situation”.

Tactics, techniques, and procedures (TTPs)

Due to the recent emergence of the group, no publicly available information exists surrounding its TTPs, including how Kairos gains initial access to organisations or how it exfiltrates data. However, phishing, and scanning for exposed internet-facing devices are common techniques used by extortion groups. Many are also known to purchase initial access from IABs on cybercriminal forums.

Associations

Kairos is not known to be associated with any other known threat groups at the time of writing. However, a user of a prominent ransomware-focused Russian-language cybercriminal forum has indicated they use the nickname “kairos” on the encrypted messaging platform Tox. This user, active on the forum since December 2023, has made several forum contributions. These include the sharing a guide for using their custom post-exploitation script called “DarkSilent” in September 2024. Their profile indicates that they are also active on other gated Russian-language cybercriminal forums.

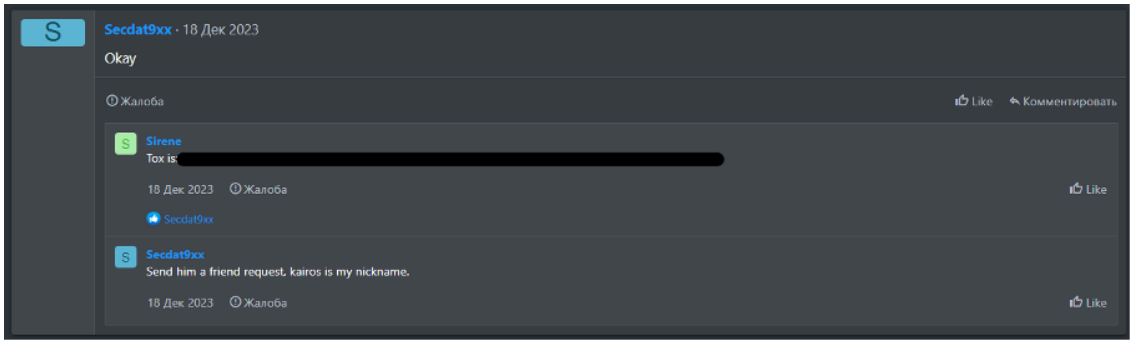

Figure 5. Cybercriminal forum user claims to use “Kairos” nickname on Tox.

Not enough information exists to confidently attribute the forum user to the Kairos extortion group at this time. However, their DarkSilent guide would potentially provide detailed insights into the group’s TTPs should they indeed be operated by one and the same entity.

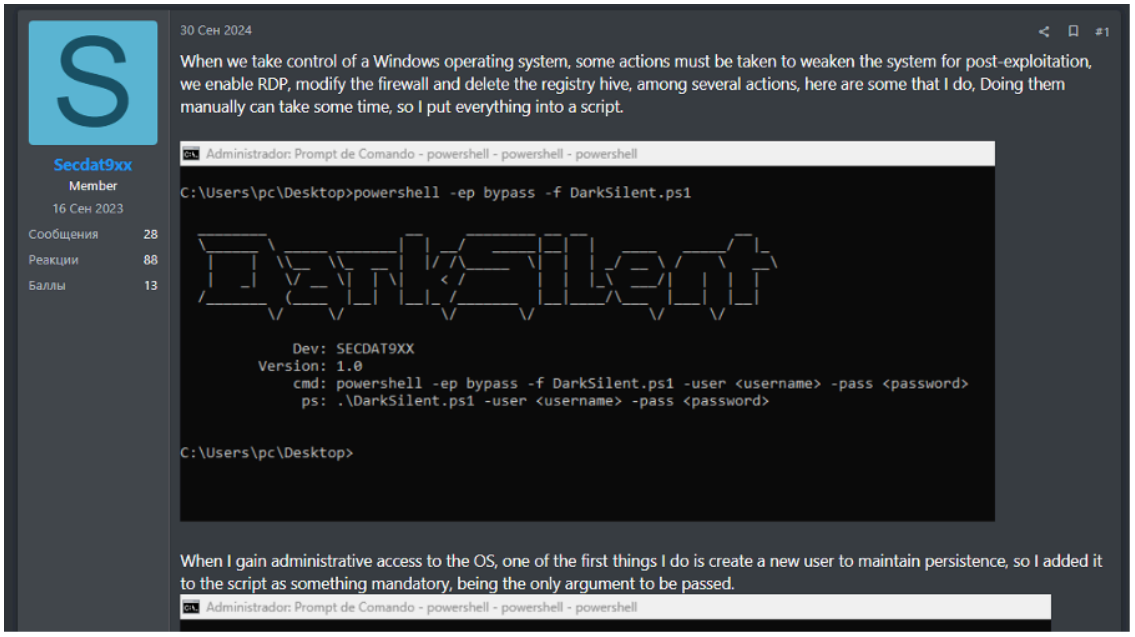

Figure 6. Potential alias for Kairos sharing script for post-exploitation on a cybercriminal forum.

Threat assessment

Kairos has claimed attacks against a small number of medium-sized businesses, mostly in the vulnerable healthcare sector. At least two of these victims have publicly confirmed data breaches earlier this year, though it is yet unclear whether these are related to Kairo’s operations. The group operates a well-functioning DLS. There are

no known concrete TTPs associated with the group at this time, and so it is unclear to what extent it is technically capable.

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.

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.

Source: https://www.cyjax.com/resources/blog/an-elephant-in-kairos-data-leak-site-emerges-for-new-extortion-group/