Take Me Down to Funksec Town: Funksec Ransomware DLS Emergence - CYJAX

By Adam Price, Ethan Spiteri

Published: 2024-12-03 · Archived: 2026-04-02 11:38:06 UTC

Cyjax has continued to observe the emergence of data-leak sites (DLSs) for extortion and ransomware groups, with ContFR, Argonauts, Kairos, Chort, and Termite, appearing November 2024 alone. Cyjax has identified the emergence of a Tor-based DLS belonging to a new, self-called "*cybercrime group*" named 'Funksec'. This group has claimed 11 victims so far and advertises a free Distributed Denial-of-Service (DDoS) tool.

Read on to find out what Cyjax knows so far about this new threat group.

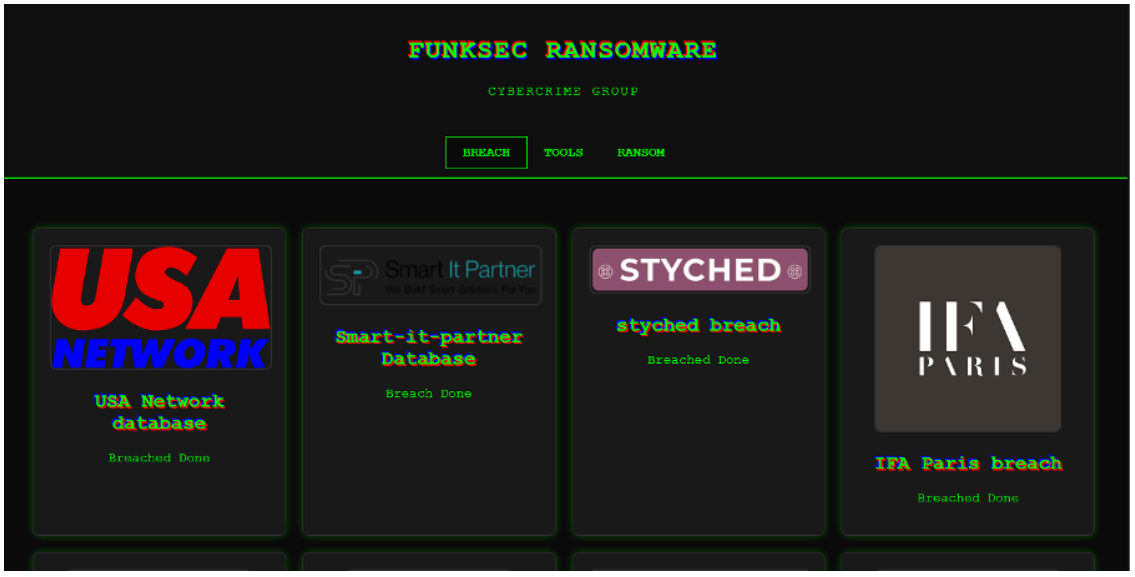

Figure 1 **–**Funksec DLS landing page.

Context

Ransomware-as-a-service operations 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. This proof may include 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 all stolen data available to DLS visitors, either for free or at cost.

Victimology

FunkSec has claimed 11 victims as of 3 December 2024, which span the media, IT, retail, education, automotive, professional services, and NGO sectors across the United States, Tunisia, India, France, Thailand, Peru, Jordan, and United Arab Emirates.

As the group is advertised as a ransomware group, and there is a "*RANSOM*" page in the DLS, it is likely that the group uses a double extortion method. This involves the group both encrypting and exfiltrating files on victim devices.

Known locations

Funksec's DLS was likely created in September 2024, and the group appears to have been active since this date. One advertisement for the DLS was shared to a cybercriminal forum on 3 December 2024.

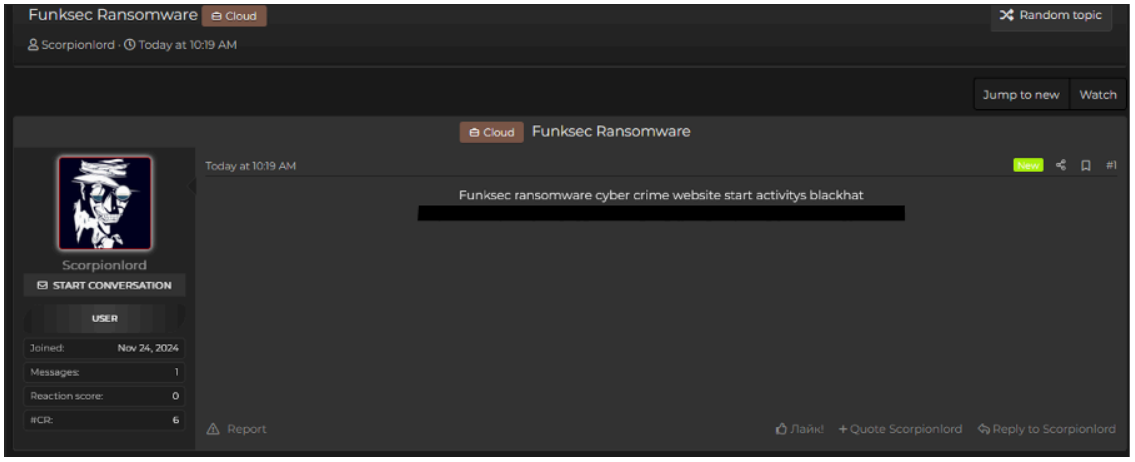

Figure 2 – Post on cybercriminal forum advertising Funksec's DLS.

The advertisement was titled "*Funksec Ransomware*", indicating that the group's main motivation is financial gain through victim extortion. It is currently unknown whether the user 'Scorpionlord' is a spokesperson of the group, an affiliate, operator, or actively involved in the attacks.

Funksec is also active on another cybercriminal forum with several users posting as early as September 2024. These users have posted data breaches attributed to "*Funksec group*" and have high reputation scores, indicating a level of credibility to the threat group and its attacks.

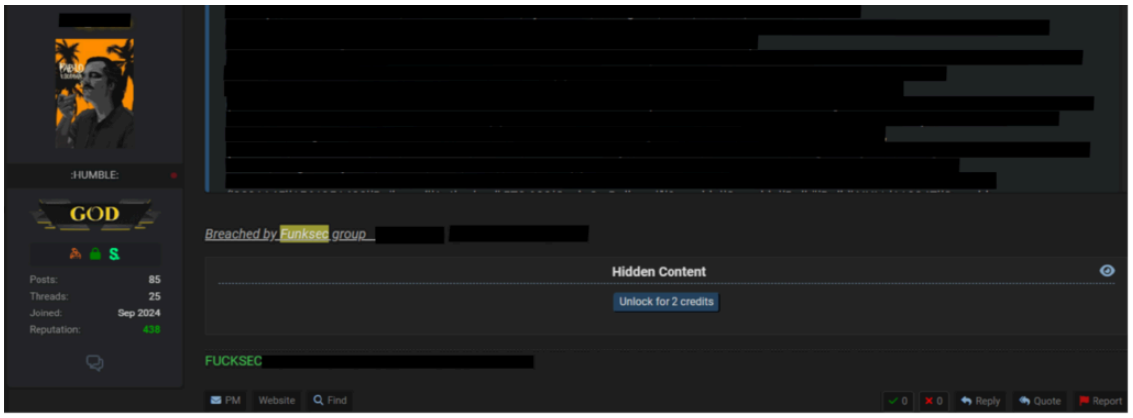

Figure 3 – Screenshot of Funksec breach post on cybercriminal forum

The DLS consists of three main pages, named "*BREACH*", "*TOOLS*", and "*RANSOM*".

BREACH (landing page)

The 'BREACH' page is the DLS' landing page, containing links to pages for each successful attack listing.

These links contain a logo or banner of the victim organisation, its name, and an indication that the breach is complete, or "*done*".

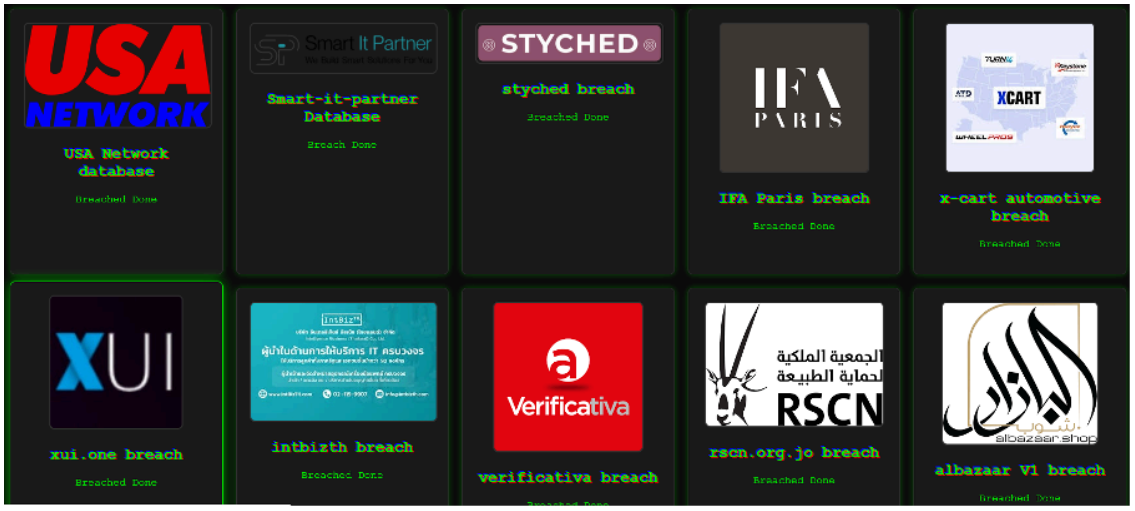

Figure 4 – Victim listings on the Funksec DLS.

RANSOM

Currently, this page does not have any content, simply stating "*comming* [sic] *soon* …". Due to the new appearance of Funksec in the threat landscape, it is highly likely that this page will be populated as the group continues to conduct ransomware attacks.

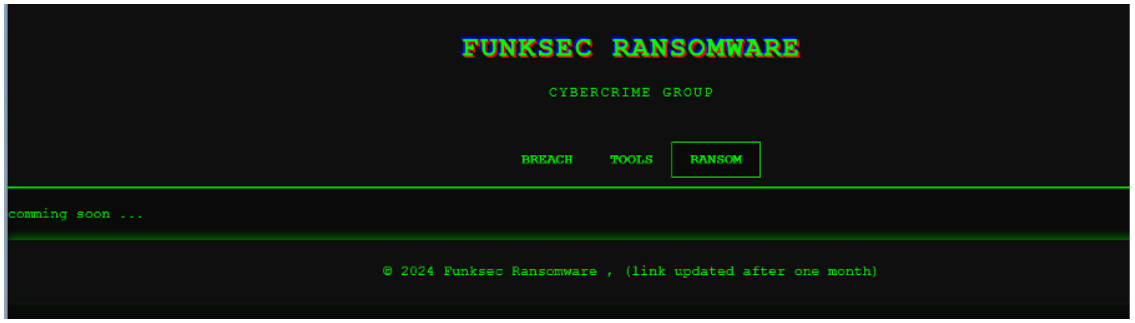

Figure 7 – "*RANSOM*" page on Funksec's DLS.

Leak listings

For listings in which the breach status is "*done*", visitors can access a page for each victim.

These pages contain further information about the victim organisation, the leaked data, and a download link for the leak. Each listing uses file sharing platforms such as fastupload and gofile, rather than a self-hosted content distribution network.

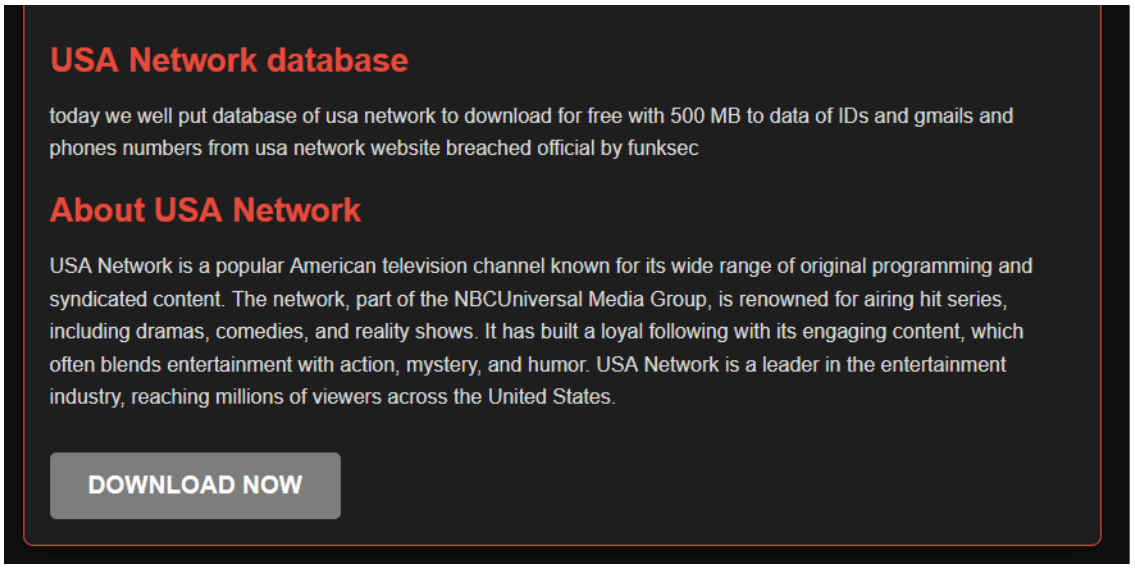

Figure 8 – Listing information page on Funksec's DLS.

Tactics, techniques, and procedures (TTPs)

Due to the recent emergence of the group, little publicly available information exists surrounding Funksec's TTPs.

The existence of data leaks implies the use of double extortion in its ransomware attacks. As the group has allegedly developed its own DDoS tool, it is realistically possible that it might use this tool in its own attacks.

No information regarding an initial access vector is known. However, ransomware groups often gain initial access through commonly used techniques such as vulnerability exploitation, brute forcing credentials, or purchasing access from initial access brokers (IABs) on cybercriminal forums.

Associations

At the time of writing, Funksec is not known to be associated with any other known threat groups. If the forum users continue to post on behalf or relating to Funksec, it is likely that they are a spokesperson or operator of the ransomware operation.

Threat assessment

Funksec appears to have significant technical capability, possibly creating its own ransomware binary and DDoS tool. There are 11 public attack announcements, and the group operates a functional Tor-based DLS to centralise its ransomware operation and post data leaks from successful attacks. As more victims are added to this DLS, the prevalence and associated threat of the group is likely to increase.

Explore our complete intelligence repository, featuring detailed profiles on extortion groups, APTs, data brokers, hacktivists, initial access brokers, and more. Click here to demo Cymon

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.
