

A white outline icon of a folder, positioned to the left of the word "BRIEF".

BRIEF

Recent RansomHouse Ransomware Gang Activity

ZEROFOX INTELLIGENCE

B-2022-05-13a

Classification: WHITE

Criticality: HIGH

Intelligence Requirements: Deep Dark Web & Criminal Underground

May 13, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 10:00 AM (EDT) on May 13, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Recent RansomHouse Ransomware Gang Activity

Executive Summary

On May 10, 2022, ZeroFox observed several updates on the RansomHouse leak site revealing multiple victims. Two of the four victims, Jefferson Credit Union and the Saskatchewan Liquor and Gaming Authority, were listed with links available to download all of their stolen data. There was no link to the data of the other two victims, AHS Aviation Handling Services and Dellner, but the site claims to have “evidence” that these entities have been breached. RansomHouse may be connected to APT group FIN8, as evidenced by shared infrastructure and malware used by the WhiteRabbit ransomware.

Analyst Commentary

Jefferson Credit Union (JCU) is an Alabama-based credit union that describes itself as “owned by ordinary people who work together as members to help each other achieve financial success and live well.”¹ RansomHouse claims to have encrypted systems at JCU on December 10, 2021, though the credit union was not listed publicly until months later. Figure 1 below shows that RansomHouse has made over two terabytes of stolen data available for download after JCU did not pay the demanded ransom. The group behind the breach criticized the credit union for its decision not to pay with a message on the victim’s page:

Jefferson Credit Union facility was notified of the data leak, but preferred to take the path of silence and money-saving instead of their clients' privacy and safety. From our side we offer individuals to contact us via our Dedicated Telegram Channel with a request to remove their personal information from disclosure. This option is available until the company's status changes to Disclosed.

¹ [https://jeffersoncreditunion\[.\]org/info-center/about-jcu/our-story/](https://jeffersoncreditunion[.]org/info-center/about-jcu/our-story/)



[Main](#) [About](#) [Rules](#) [FAQ](#)

Jefferson Credit Union "Jefferson Credit Union is owned by ordinary people..." - wow, nothing to add here really. <table><tr><td>Website https://www.jeffersoncreditunion.org</td><td>Revenue \$26M</td><td>Employees 126</td></tr></table>	Website https://www.jeffersoncreditunion.org	Revenue \$26M	Employees 126	Encrypted 10/12/2021 Downloaded more than 2Tb Status: DISCLOSED 26/04/2022 141	Share Contact us
Website https://www.jeffersoncreditunion.org	Revenue \$26M	Employees 126			

FULL DATA DUMP: [Download](#) **Password:** no password

Figure 1. Jefferson Credit Union's victim listing on the RansomHouse leak site

Source: ZeroFox Intelligence

Saskatchewan Liquor and Gaming Authority (SLGA), a Canadian state-owned corporation responsible for the distribution, control, and regulation of alcoholic beverages, cannabis, and gambling facilities in the Canadian province of Saskatchewan, was also listed publicly on May 10, 2022. Similarly to JCU, SLGA's listing on the RansomHouse leak site took several months; the attack was described as having occurred on December 20, 2021. SLGA published a press release just eight days later, notifying the public that it had been subject to a cyber security incident. Roughly two terabytes of SLGA data was stolen and made available for download.²

Dellner is a supplier of train connection systems dealing in couplers, gangways, front hatches, dampers, and crash energy management. Based in Sweden, Dellner has 22 subsidiaries across the globe with more than 1,200 employees. RansomHouse claims to have encrypted Dellner's systems on April 8, 2022, and stolen around one terabyte of data. As of May 10, 2022, this data has yet to be made available for download.

AHS Aviation Handling Services describes itself as "the market leader in Germany among the airline-independent providers in the field of passenger handling and operations."³ The AHS Group serves 130 airlines at major German airports. RansomHouse claims to have encrypted The AHS Group on April 16, 2022, stealing more than four terabytes of data. Although RansomHouse provided an "evidence pack," the full set of stolen data has not been made available.

²

<https://www.saskatchewan.ca/government/news-and-media/2021/december/28/cyber-security-incident-at-slga>

³ <https://www.ahs-de.com/ueber-uns>



[Main](#) [About](#) [Rules](#) [FAQ](#)

AHS Aviation Handling Services GmbH The AHS Group is the market leader in Germany among independent providers of airline passenger handling and operations. Website https://www.ahs-de.com Revenue \$658M Employees 3255	Encrypted 16/04/2022 Downloaded more than 4Tb	Share Contact us
163 Status: EVIDENCE 16/04/2022		
Evidence packs: Download Password: x5CLG6aPE1YtC3UzuwpX		

Figure 2. RansomHouse claims to have stolen more than four terabytes of data from The AHS Group

Source: ZeroFox Intelligence

The WhiteRabbit ransomware may be connected to the RansomHouse leak site, as indicated by the phrase “Welcome to the Ransom House” contained in ransom notes attributed to this group. Researchers from Lodestone have also potentially connected this recent ransomware family to FIN8 through the URL used and WhiteRabbit’s use of a previously-unseen version of the BADHATCH backdoor.⁴ FIN8 is a financially-motivated APT threat group known to launch spear phishing campaigns against retail, restaurant, and hospitality industries.

⁴ [hXXps://lodestone\[.\]com/insight/white-rabbit-ransomware-and-the-f5-backdoor/](https://lodestone[.]com/insight/white-rabbit-ransomware-and-the-f5-backdoor/)



```
-----
HELLO [REDACTED]
If you are reading this message, means that:
- your network infrastructures have been compromised,
- critical data has leaked,
- files are encrypted

a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"
a"f Welcome to the Ransom House a"
a"f You are locked by a"
a"f W H I T E R A B B I T a"
a"f Knock, Knock. Follow the white Rabbit... a"
a"f
a"f { \ /
a"f { ~ - ~
a"f { " " }
a"
a"-a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"
The best and only thing you can do is to contact us
to settle the matter before any losses occurs.

-----

1. THE FOLLOWING IS STRICTLY FORBIDDEN

1.1 DELETION THIS NOTE.      Each note carries the encryption key
                             needed to decrypt the data,
                             don't lose it
```

Figure 3. A partial ransom note dropped by WhiteRabbit ransomware

Source:

[hXXps://www.trendmicro\[.\]com/en_us/research/22/a/new-ransomware-spotted-white-rabbit-and-its-evasion-tactics.html](https://www.trendmicro.com/en_us/research/22/a/new-ransomware-spotted-white-rabbit-and-its-evasion-tactics.html)

ZeroFox Intelligence has detected more than 4,000 victims of ransomware and digital extortion in the last year. Nearly 50 percent of these victims were in the U.S.-Canada region, while close to 30 percent of observed victims were in the Europe-Russia region. Over 250 ZeroFox Intelligence-observed victims were connected to the financial services sector. The logistics sector saw more than 200 victims of ransomware in the last year.



Appendix: Traffic Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:

RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:

RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:

AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:

GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP:

WHITE information without restriction, subject to copy-right controls.