Report for 970094589513982043’s (nekomataonigiri.) server being hack and discord token being lack

HN Hosting, Operation Team

HYPER GROUP NETWORK LTD | INFO@HYPERNITE.COM

Reason for the item,

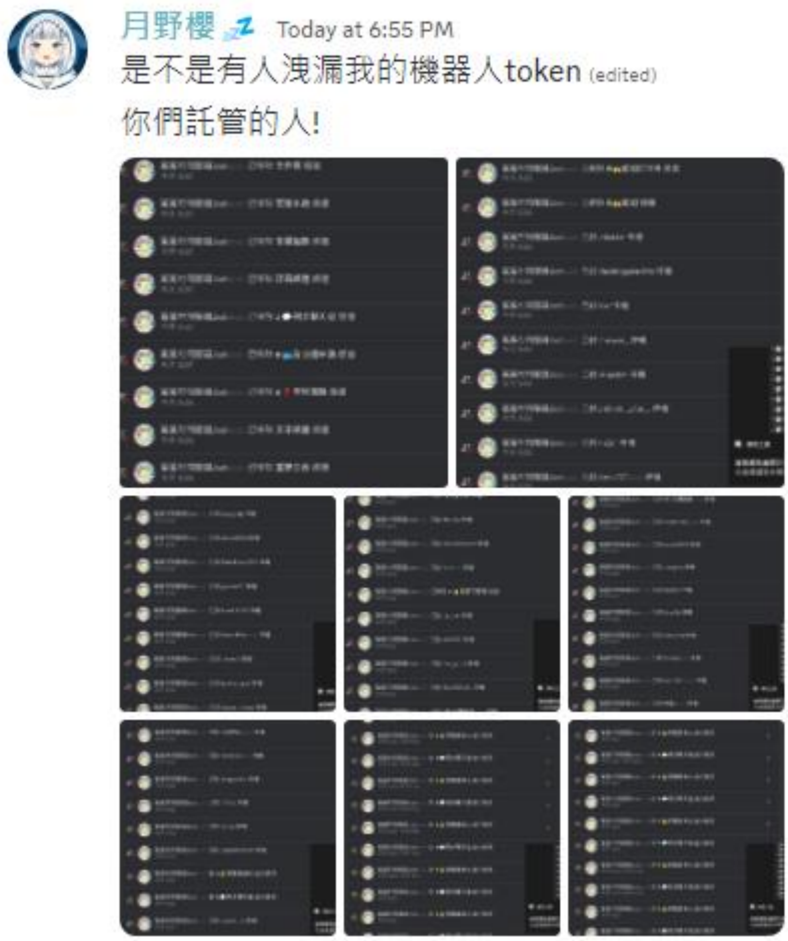
To confirm the hack is not related to HN internal policy and staff and define the responsibility of this attack.

Roles:

- Chief Administration Officer – Issac Li (Report Drafter)
- Chief Technology Officer – Anson Tsang (Technical Specification)
- Chief Information and Operation Officer (Operation Specification)
- Lead of HN Trust and Safety - Taddeo Leung (Report Verifier)
- The lead of Human Resources and Administration - Owen Liu (Report Verifier)

Complain from,

- Location: Discord
- Channel: 1080504136954544128, 1164882421074903061
- Server: 200144348891971584
- Reported User: nekomataonigiri.(970094589513982043)



月野櫻 💤 Today at 6:55 PM

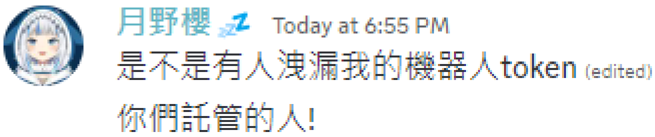
是不是有人洩漏我的機器人token (edited)

你們託管的人!

Investigation Description:

- 20 Oct 2023

At 18:55, user nekomataonigiri. (AKA reporter) claimed that our staff leaked the token about his discord bot, leading to his server being “discord raid”. (As captured below)

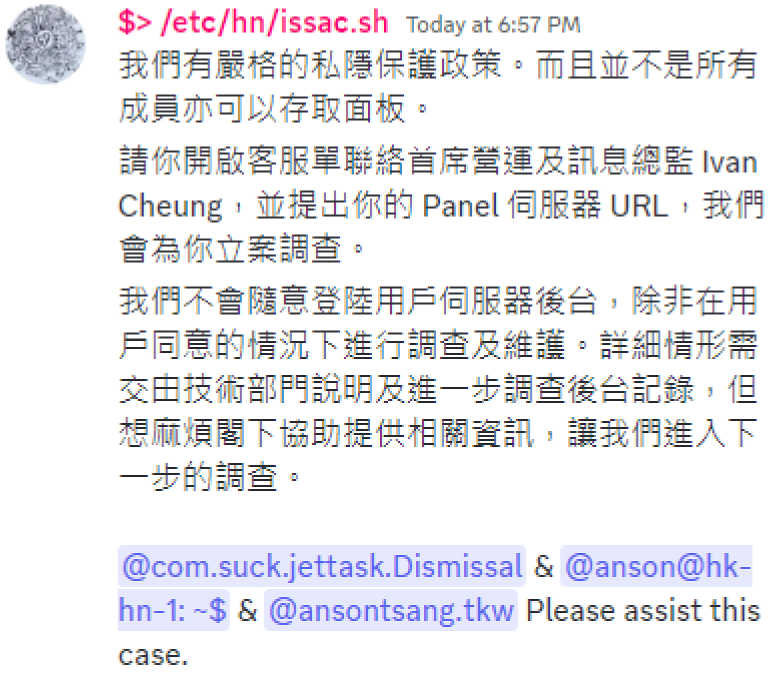


月野櫻 Today at 6:55 PM

是不是有人洩漏我的機器人token (edited)

你們託管的人!

CAO, Issac Li has replied that HN (Hyper Group) defined a privacy policy and not all staff can access the host panel (https://panel.hnhost.net). CAO advised the user to open a ticket and contain our COIO, Ivan Cheung and provide the URL about the panel to perform further investigation. CAO also claimed that we, as Hyper Group staff, will not access the server panel backend without any permission and requested the user to provide the information for further investigation. CAO request CTO, COIO and Operation Lead to support this case.



$> /etc/hn/issac.sh Today at 6:57 PM

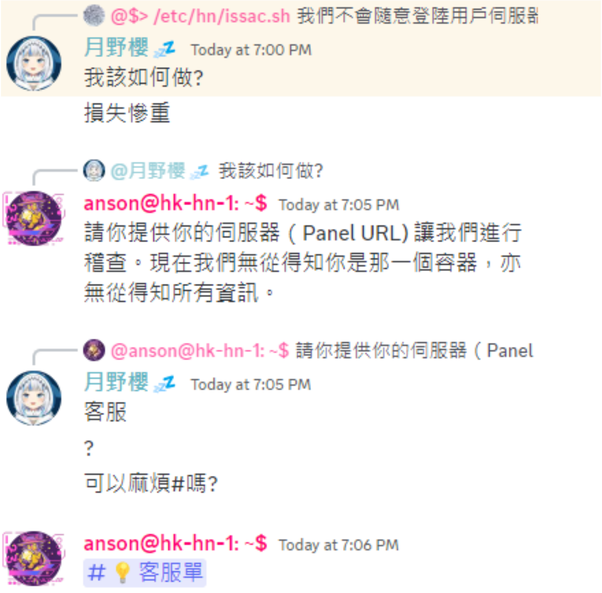
我們有嚴格的私隱保護政策。而且並不是所有成員亦可以存取面板。

請你開啟客服單聯絡首席營運及訊息總監 Ivan Cheung，並提出你的 Panel 伺服器 URL，我們會為你立案調查。

我們不會隨意登陸用戶伺服器後台，除非在用戶同意的情況下進行調查及維護。詳細情形需交由技術部門說明及進一步調查後台記錄，但想麻煩閣下協助提供相關資訊，讓我們進入下一步的調查。

@com.suck.jettask.Dismissal & @anson@hk-hn-1: ~$ & @ansontsang.tkw Please assist this case.

CTO, Anson Tsang has requested the user to provide the information and the user opened a ticket at 19:06.



@$> /etc/hn/issac.sh 我們不會隨意登陸用戶伺服器

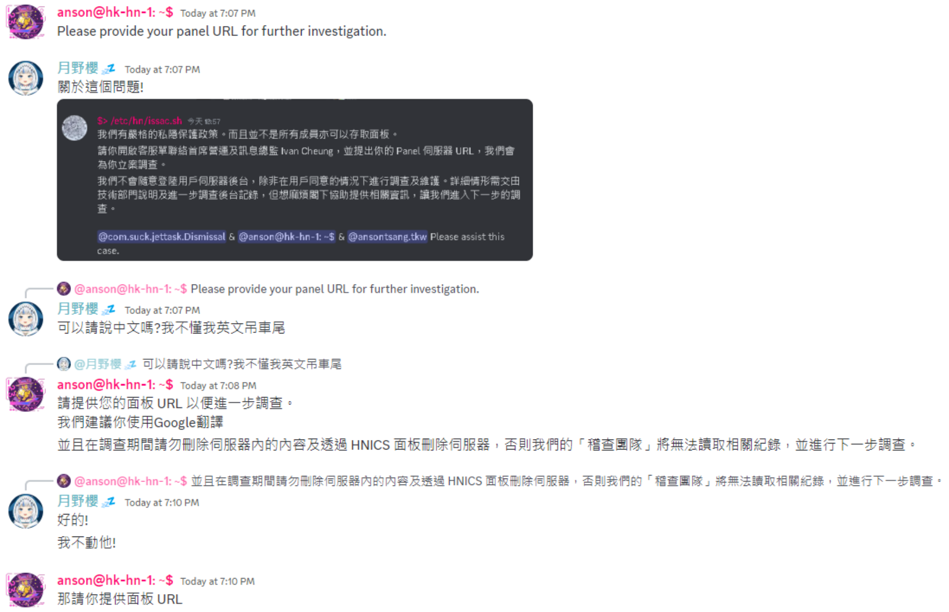
月野櫻 Today at 7:00 PM
我該如何做?
損失慘重

@月野櫻 我該如何做?
anson@hk-hn-1: ~$ Today at 7:05 PM
請你提供你的伺服器（Panel URL）讓我們進行稽查。現在我們無從得知你是那一個容器，亦無從得知所有資訊。

@anson@hk-hn-1: ~$ 請你提供你的伺服器（Panel
月野櫻 Today at 7:05 PM
客服
?
可以麻煩#嗎?

anson@hk-hn-1: ~$ Today at 7:06 PM
💡 客服單

CTO requested the reporter to provide the server URL again and he claimed that he didn’t know English and could not communicate with us. CTO changed the reply language to Chinese. The CTO requested the reporter to provide the server URL multiple times but failed.



anson@hk-hn-1: ~$ Today at 7:07 PM
Please provide your panel URL for further investigation.

月野櫻 Today at 7:07 PM
關於這個問題!

$> /etc/hn/issac.sh 今天 18:57
我們有嚴格的私隱保護政策。而且並不是所有成員亦可以存取面板。
請你開啟客服單聯絡首席營運及訊息總監 Ivan Cheung，並提出你的 Panel 伺服器 URL，我們會為你立案調查。
我們不會隨意登陸用戶伺服器後台，除非在用戶同意的情況下進行調查及維護。詳細情形需交由技術部門說明及進一步調查後台記錄，但想麻煩閣下協助提供相關資訊，讓我們進入下一步的調查。

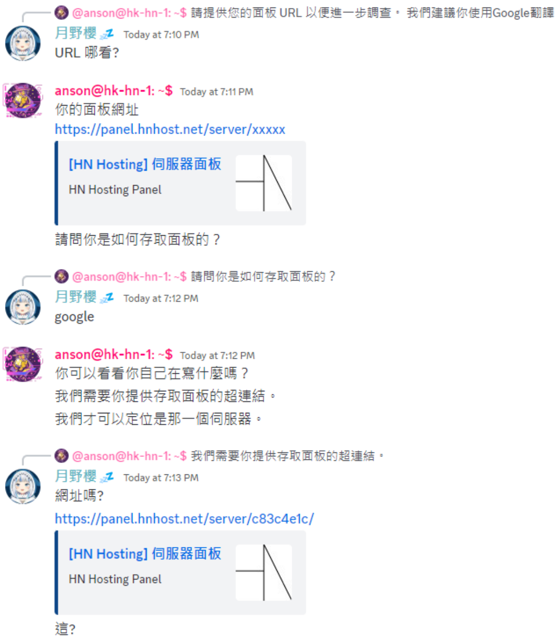
@com.suck.jettask.Dismissal & @anson@hk-hn-1: ~$ & @ansontsang.tkw Please assist this case.

@anson@hk-hn-1: ~$ Please provide your panel URL for further investigation.
月野櫻 Today at 7:07 PM
可以請說中文嗎?我不懂我英文吊車尾

@月野櫻 可以請說中文嗎?我不懂我英文吊車尾
anson@hk-hn-1: ~$ Today at 7:08 PM
請提供您的面板 URL 以便進一步調查。
我們建議你使用Google翻譯
並且在調查期間請勿刪除伺服器內的內容及透過 HNICS 面板刪除伺服器，否則我們的「稽查團隊」將無法讀取相關紀錄，並進行下一步調查。

@anson@hk-hn-1: ~$ 並且在調查期間請勿刪除伺服器內的內容及透過 HNICS 面板刪除伺服器，否則我們的「稽查團隊」將無法讀取相關紀錄，並進行下一步調查。
月野櫻 Today at 7:10 PM
好的!
我不動他!

anson@hk-hn-1: ~$ Today at 7:10 PM
那請你提供面板 URL



@anson@hk-hn-1: ~$ 請提供您的面板 URL 以便進一步調查。 我們建議你使用Google翻譯

月野櫻 Today at 7:10 PM

URL 哪看?

anson@hk-hn-1: ~$ Today at 7:11 PM

你的面板網址

https://panel.hnhost.net/server/xxxxx

[HN Hosting] 伺服器面板

HN Hosting Panel

請問你是如何存取面板的？

@anson@hk-hn-1: ~$ 請問你是如何存取面板的？

月野櫻 Today at 7:12 PM

google

anson@hk-hn-1: ~$ Today at 7:12 PM

你可以看看你自己在寫什麼嗎？

我們需要你提供存取面板的超連結。

我們才可以定位是那一個伺服器。

@anson@hk-hn-1: ~$ 我們需要你提供存取面板的超連結。

月野櫻 Today at 7:13 PM

網址嗎?

https://panel.hnhost.net/server/c83c4e1c/

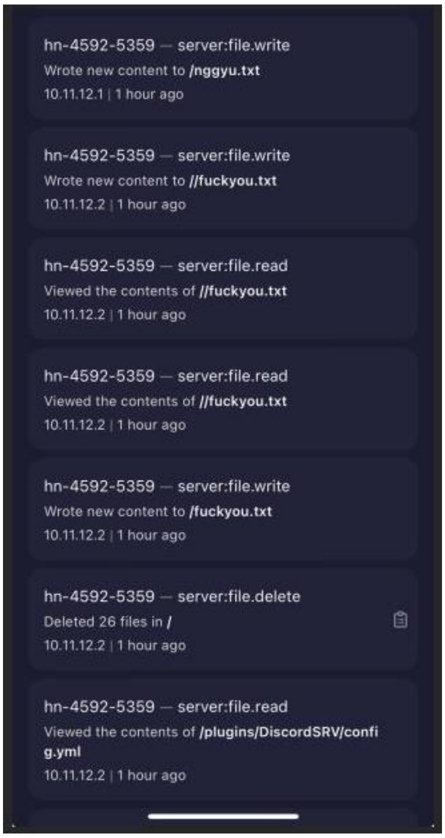
[HN Hosting] 伺服器面板

HN Hosting Panel

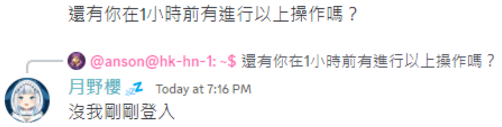
這?

At 19:13, the reporter finally provided the server URL to the CTO and the investigation started.

AT 19:16, the CTO discovered suspicious access and action performed at the server “c83c4e1c” and reported to the reporter and confirmed if those actions were performed by the reporter himself.



```
hn-4592-5359 — server:file.write
Wrote new content to /nggyu.txt
10.11.12.1 | 1 hour ago

hn-4592-5359 — server:file.write
Wrote new content to //fuckyou.txt
10.11.12.2 | 1 hour ago

hn-4592-5359 — server:file.read
Viewed the contents of //fuckyou.txt
10.11.12.2 | 1 hour ago

hn-4592-5359 — server:file.read
Viewed the contents of //fuckyou.txt
10.11.12.2 | 1 hour ago

hn-4592-5359 — server:file.write
Wrote new content to /fuckyou.txt
10.11.12.2 | 1 hour ago

hn-4592-5359 — server:file.delete
Deleted 26 files in /
10.11.12.2 | 1 hour ago

hn-4592-5359 — server:file.read
Viewed the contents of /plugins/DiscordSRV/confi
g.yml
10.11.12.2 | 1 hour ago
```



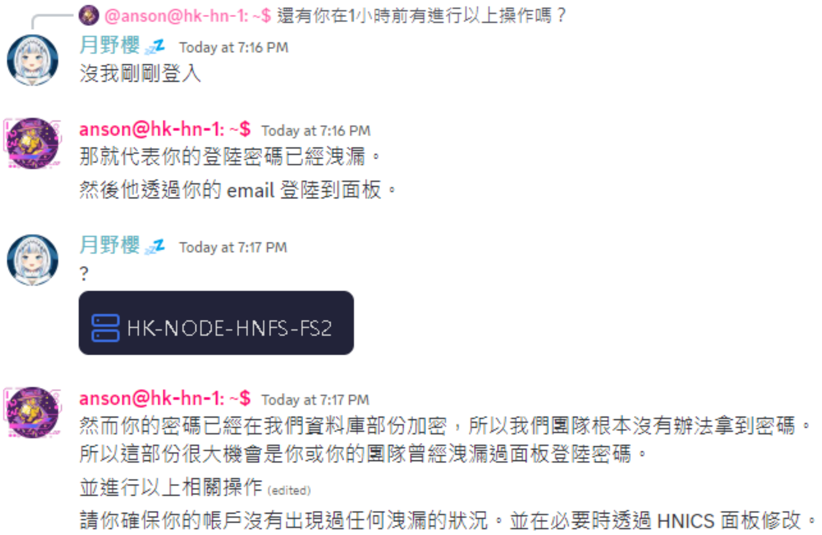
還有你在1小時前有進行以上操作嗎？

@anson@hk-hn-1: ~$ 還有你在1小時前有進行以上操作嗎？

月野櫻 Today at 7:16 PM

沒我剛剛登入

At 19:16, the CTO replied this means the panel password is leaked and the hacker access the panel via the registered email and password leaked. The CTO also notified our password is encrypted in our own database and our staff were not able to obtain the password by accessing the database.



@anson@hk-hn-1: ~$ 還有你在1小時前有進行以上操作嗎？

月野櫻 Today at 7:16 PM
沒我剛剛登入

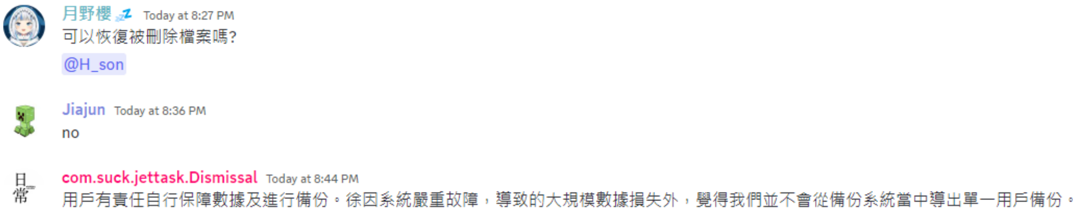
anson@hk-hn-1: ~$ Today at 7:16 PM
那就代表你的登陸密碼已經洩漏。
然後他透過你的 email 登陸到面板。

月野櫻 Today at 7:17 PM
?
HK-NODE-HNFS-FS2

anson@hk-hn-1: ~$ Today at 7:17 PM
然而你的密碼已經在我們資料庫部份加密，所以我們團隊根本沒有辦法拿到密碼。
所以這部份很大機會是你或你的團隊曾經洩漏過面板登陸密碼。
並進行以上相關操作 (edited)
請你確保你的帳戶沒有出現過任何洩漏的狀況。並在必要時透過 HNICS 面板修改。

At 20:27, the user requested to restore the lost files. RAD Manager, Jia Jun replied it was not possible to restore and the COIO was notified user had the responsibility to protect his own data and perform a backup if necessary.

Overall case and description ended.



月野櫻 Today at 8:27 PM
可以恢復被刪除檔案嗎?
@H_son

Jiajun Today at 8:36 PM
no

com.suck.jettask.Dismissal Today at 8:44 PM
用戶有責任自行保障數據及進行備份。徐因系統嚴重故障，導致的大規模數據損失外，覺得我們並不會從備份系統當中導出單一用戶備份。

Conclusion,

Hyper Group do not have the responsibility in this case as we already notified user should perform their backup regularly and none of our staff is included in this Raid attack.

Recommendation,

Users should keep their own passwords safe and notify HN staff immediately if unknown access happens.