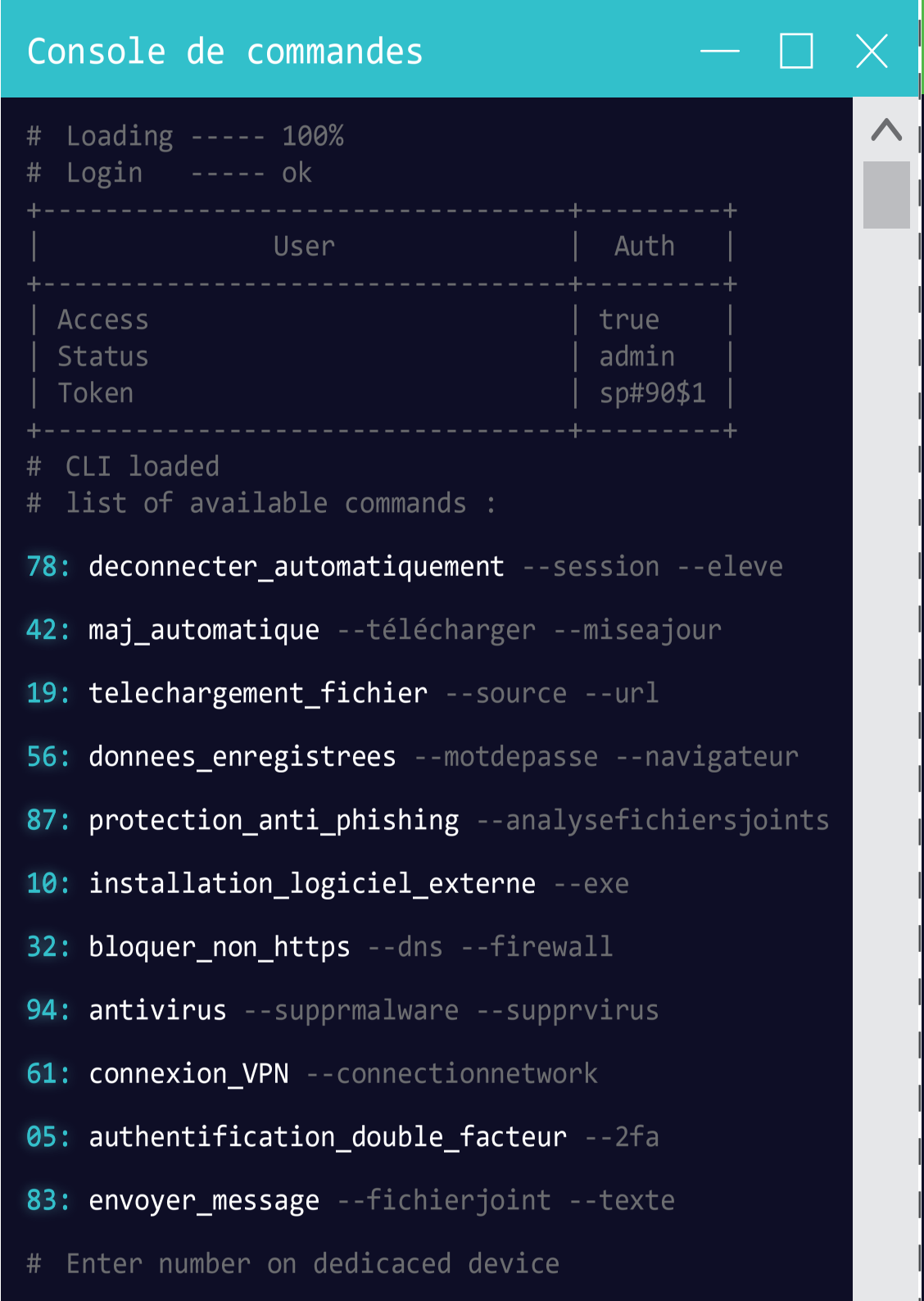
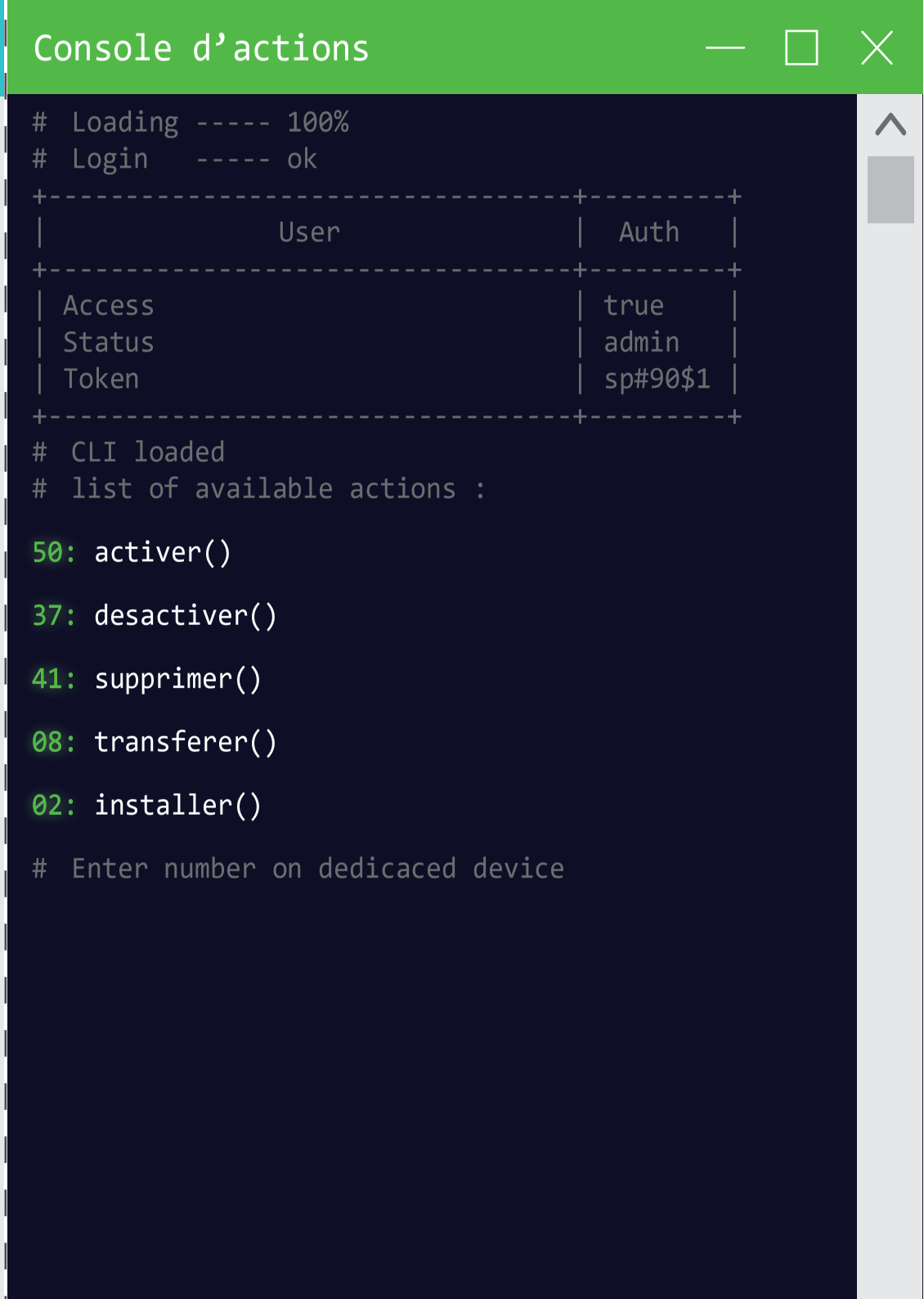

Console de commandes
Loading ----- 100%
Login ----- ok
+----------+
| User | Auth |
+----------+
Access	true
Status	admin
Token	sp#90$1
+----------+
CLI loaded
list of available commands :
78: deconnecter_automatiquement --session --eleve
42: maj_automatique --télécharger --miseajour
19: telechargement_fichier --source --url
56: donnees_enregistrees --motdepasse --navigateur
87: protection_anti_phishing --analysefichiersjoints
10: installation_logiciel_externe --exe
32: bloquer_non_https --dns --firewall
94: antivirus --supprmalware --supprvirus
61: connexion_VPN --connectionnetwork
05: authentification_double_facteur --2fa
83: envoyer_message --fichierjoint --texte
Enter number on dedicaced device


Console d'actions
Loading ----- 100%
Login ----- ok
+----------+
| User | Auth |
+----------+
Access	true
Status	admin
Token	sp#90$1
+----------+
CLI loaded
list of available actions :
50: activer()
37: desactiver()
41: supprimer()
08: transferer()
02: installer()
Enter number on dedicaced device

OUTILS

Console des actions

OUTILS

Console des commandes

A - Stockage mots de passe :

Il ne faut jamais enregistrer des données sensibles comme des codes bancaires ou des mots de passe dans son navigateur. Dans cette situation, supprimez immédiatement les données en cache et les mots de passe enregistrés, puis cherchez une alternative sécurisée.

B - Mise à jour logiciel :

Mettre à jour ses logiciels est indispensable pour assurer un haut niveau de sécurité. Attention, dans certains cas les logiciels sont vulnérables si les mises à jour ne sont pas faites. Pensez à des solutions comme la mise à jour automatique en cas de besoin.

C - Ne pas se déconnecter :

Ne pas se déconnecter de son compte ou de sa session est un problème courant, mais potentiellement grave. N'importe qui peut accéder très facilement à vos données. La déconnexion automatique permet d'éviter ce genre de problème.

CARTE OUTIL
GUIDE DE BONNES PRATIQUES

D - Le téléchargement de fichiers douteux :

Il existe un risque qu'elle contienne un « stealer », un virus visant à dérober des données. Bloquer les téléchargements en attendant de résoudre le problème est une solution radicale mais efficace.

E - L'hameçonnage :

Aussi appelé « phishing », c'est une technique destinée à leurrer l'utilisateur pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance. Il est souvent utilisé dans un mail ou un sms essayant de paraître urgent et officiel. La meilleure solution est d'installer une protection et d'être attentif.

F - Le dérobeur :

Aussi appelés « stealers », ces virus sont spécialisés dans le vol d'identifiants et de mots de passe, de portefeuille, ou d'informations type cookie. Ces virus se cachent souvent dans des éléments à télécharger, visant à donner envie. Exemple: un jeu vidéo, une vidéo exclusive... Pour pousser certains utilisateurs à télécharger le contenu.

OUTILS

Guide des Bonnes Pratiques

page #1

OUTILS

Guide des Bonnes Pratiques

page #2

G - Gestionnaire de mots de passe sécurisés :

Un gestionnaire de mots de passe sécurisé est comme votre gardien numérique personnel. Il stocke vos mots de passe de manière chiffrée. C'est une solution courante, mais d'autres existent autant en ligne que stocké dans l'ordinateur.

H - Antivirus :

L'antivirus est le bouclier numérique de votre appareil. Il surveille en permanence votre système à la recherche de menaces telles que virus, pourriciels (ou malwares) et logiciels malveillants.

I - Adresse IP :

Une adresse IP est un numéro d'identification unique que vos appareils utilisent pour se connecter à Internet (PC, tablette, smartphone, objet connecté..). C'est comme une plaque d'immatriculation qui indique où se trouve votre appareil sur le réseau. Une adresse IP est comprise entre 0.0.0.1 et 255.255.255.255.

CARTE OUTIL
GUIDE DE BONNES PRATIQUES

J - Double authentification :

Quand cette option est disponible, activez-la. Doubler la vérification de votre identité est une sécurité cruciale, notamment concernant les paiements en ligne. Consultez les paramètres de sécurité de l'application pour savoir si cette option est disponible.

K - Hyper Text Transfer Protocol Secure

Le HTTPS est comme une lettre scellée lorsqu'on l'envoie par la poste. Il sécurise la communication entre votre navigateur et le site Web que vous visitez. Par contre, cela ne permet pas d'authentifier l'émetteur car les escrocs peuvent également l'utiliser.

L - Virtual Private Network :

Le VPN crée une connexion chiffrée, protégeant vos données des regards indiscrets. Utiliser un VPN garantit une navigation anonymisée et sécurisée, même sur un réseau public.

OUTILS

Guide des Bonnes Pratiques

page #3

OUTILS

Guide des Bonnes Pratiques

page #4