aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de novembre 2022

2022-11-30 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse

Ce mois-ci, certaines vulnérabilités critiques comme celles d'*OpenSSL* étaient considérées **prioritaires** dans le cadre du maintien en condition de sécurité des systèmes d'information. Ce bulletin décline cinq autres failles à ne pas négliger dans l'analyse des risques de son infrastructure.

Malgré un correctif livré avec le ***Patch Tuesday*** de novembre, une nouvelle vulnérabilité affectant le dispositif *MoTW* est apparue comme largement exploitée lors de récentes campagnes d'attaques, comme celle de Qakbot.

L'actualité a encore démontré l'activité soutenue des groupes de *Ransomware* : l'affaire Thales (groupe Lockbit 3.0), le département des Alpes-Maritimes, l'entreprise française ITS Group, tous deux ciblés par le groupe PLAY.

Les dirigeants et employés des entreprises victimes de cyberattaques, sont soumis à un haut niveau de stress. Un guide d'accompagnement vous est proposé pour vous assister lors de la gestion d'une crise.

2. Les CVE de novembre

Ce mois-ci, le CERT aDvens met en exergue cinq vulnérabilités en raison de leur large utilisation au sein des entreprises, leurs risques et leur exploitation.

L'application de leurs correctifs ou contournements est fortement recommandée.

Les failles critiques CVE-2022-3602 et CVE-2022-3786 affectant ***OpenSSL***, ne sont pas présentées dans cet article, en raison d'une publication d'un bulletin d'alerte par le CERT aDvens le 09 novembre.

2.1. Google Chrome - CVE-2022-4135

Figure 1. CVE-2022-4135

Une faille zéro-day dans Google a été découverte le 22 novembre par Clement Lecigne du *Threat Analysis Group* de Google.

Cette vulnérabilité, de type Buffer-Overflow, affectant le GPU de Google Chrome permet à un attaquant distant, via une page html forgée, de s'évader d'une *sandbox*, provoquer un déni de service ou exécuter du code arbitraire.

Les navigateurs ***Chromium*** sont aussi affectés par cette vulnérabilité.

Cette vulnérabilité est exploitée.

2.2. Informations

2.2.1. Risque

- Changement de contexte.
- Déni de service.
- Exécution de code arbitraire à distance.

2.2.2. Type de vulnérabilité

- **CWE-122**: Heap-based Buffer Overflow.

2.2.3. Criticité

Vecteur d'attaque : Réseau	Interaction de l'utilisateur : Oui	Impact sur l'intégrité : Fort
Complexité d'attaque : Faible	Portée : Changée	Impact sur la disponibilité : Fort
Privilèges requis : Aucun	Impact sur la confidentialité : Fort	

2.2.4. Composants vulnérables

- Google Chrome versions antérieures à 107.0.5304.121.
- Les navigateurs Chromium.

2.2.5. Recommandations

- Mettre à jour Google Chrome vers la version 107.0.5304.121 ou supérieure sur Mac et Linux.
- Mettre à jour Google Chrome vers la version 107.0.5304.121/122 ou supérieure sur Windows.
- Mettre à jour les navigateurs Chromium vers la dernière version.
- Plus d'informations disponibles sur le site de l'éditeur.

2.3. Atlassian Bitbucket Server & Data Center - CVE-2022-43781

Figure 2. CVE-2022-43781

Le 16 novembre 2022, l'éditeur de logiciel Atlassian publie un bulletin de sécurité sous la référence *BSERV-13522*, concernant une vulnérabilité critique de type *injection de commandes*, impactant les solutions ***Bitbucket Server*** et ***Data Center***.

Cette faille résulte d'un défaut de contrôle des données saisies par l'utilisateur lorsqu'il modifie son nom d'utilisateur. Dès que le paramètre *Allow public signup* est activé, un attaquant distant et non authentifié peut exécuter du code arbitraire sur le système.

2.4. Informations

2.4.1. Risque

- Exécution de code arbitraire à distance.

2.4.2. Type de vulnérabilité

- **CWE-78**: Improper Neutralization of Special Elements used in an OS Command (*OS Command Injection*).

2.4.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Faible	Portée: Inchangée	Impact sur la disponibilité: Fort
Privilèges requis: Aucun	Impact sur la confidentialité: Fort	

2.4.4. Composants vulnérables

Les versions suivantes sont vulnérables :

- 7.0.0 à 7.6.19 (7.6.19 exclue).
- 7.7.0 à 7.17.12 (7.17.12 exclue).
- 7.18.0 à 7.21.6 (7.21.6 exclue).
- 7.22.0 à 8.0.5 (8.0.5 exclue).
- 8.1.0 à 8.1.5 (8.1.5 exclue).
- 8.2.0 à 8.2.4 (8.2.4 exclue).
- 8.3.0 à 8.3.3 (8.3.3 exclue).
- 8.4.0 à 8.4.2 (8.4.2 exclue).

2.4.5. Recommandations

Appliquer la mise à jour vers les versions suivantes ou toutes autres versions ultérieures:

- 7.6.19 / 7.17.12 / 7.21.6.
- 8.0.5 / 8.1.5 / 8.2.4 / 8.3.3 / 8.4.2.

Pour atténuer le risque, il est recommandé de désactiver le paramètre ***Allow public signup*** dans les instances *Bitbucket Server* et *Data Center*.

Le 25 novembre, le chercheur en sécurité ***Petrus Viet*** publie sur son blog un démonstrateur exploitant la vulnérabilité.

Des informations complémentaires sont disponibles sur le bulletin de sécurité de l'éditeur.

2.5. Atlassian Crowd - CVE-2022-43782

Figure 3. CVE-2022-43782

Un second bulletin de sécurité, *BSERV-13522*, a été publié le même jour par Atlassian affectant sa solution ***Crowd***.

Crowd est un outil d'authentification unique et de gestion des identités utilisateurs. Il permet de gérer ces utilisateurs à partir de plusieurs répertoires (*Microsoft Azure AD*, *Active Directory*, *LDAP*, ou *OpenLDAP*), et de centraliser le contrôle des permissions d'authentification des applications.

Un défaut de configuration dans l'API REST, permet à un attaquant de contourner la politique de sécurité du système et d'exécuter du code arbitraire.

L'exploitation de la faille implique que l'attaquant, distant et non authentifié, accède depuis une adresse **IP autorisée**. Le défaut de configuration permet de contourner une vérification de mot de passe et de s'authentifier avec un compte de services *Crowd*. Ainsi l'attaquant peut accéder aux terminaux privilégiés de l'API REST, via la ressource *usermanagement*, et compromettre l'application.

L'exploitation de la vulnérabilité n'est possible que si l'adresse IP utilisée par l'attaquant est présente dans la liste des adresses autorisées (***Crowd's Allow List***). Par défaut, cette liste est vide.

2.6. Informations

2.6.1. Risque

- Exécution de code arbitraire à distance.
- Contournement de la politique de sécurité.

2.6.2. Type de vulnérabilité

- **CWE-284**: Improper Access Control.
- **CWE-287**: Improper Authentification.

2.6.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Faible	Portée: Inchangée	Impact sur la disponibilité: Fort
Privilèges requis: Aucun	Impact sur la confidentialité: Fort	

2.6.4. Composants vulnérables

Les versions suivantes sont vulnérables :

- 3.x.x.
- 4.x.x à 4.4.4.
- 5.x.x à 5.0.3.

2.6.5. Recommandations

Appliquer la mise à jour ***Atlassian Crowd*** vers les versions suivantes ou toutes autres versions ultérieures:

- 4.4.4.
- 5.0.3.

Si les correctifs ne peuvent pas être appliqués, il est recommandé de supprimer ou valider toutes les adresses distantes.

L'éditeur recommande d'utiliser des mots de passe robustes.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

2.7. Zyxel - CVE-2022-40602

Figure 4. CVE-2022-40602

Des chercheurs du groupe *RE-Solver*, en collaboration avec la société *Zyxel*, ont étudié une vulnérabilité critique qui affecte le routeur *LTE3301-M209*.

L'étude révèle que l'utilisation d'un mot de passe préconfiguré et incorrect, permet de contourner la politique de sécurité. Un attaquant distant et non authentifié peut exploiter cette vulnérabilité afin de s'octroyer un accès non autorisé au routeur.

L'exploitation de cette vulnérabilité est possible seulement si l'administration à distance a été activée par un administrateur authentifié.

2.8. Informations

2.8.1. Risque

- Contournement de la politique de sécurité.

2.8.2. Type de vulnérabilité

- **CWE-284**: Improper Access Control.
- **CWE-287**: Improper Authentification.

2.8.3. Criticité

Vecteur d'attaque : Réseau	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Fort
Complexité d'attaque : Faible	Portée : Inchangée	Impact sur la disponibilité : Fort
Privilèges requis : Aucun	Impact sur la confidentialité : Fort	

2.8.4. Composants vulnérables

Le logiciel du routeur ***LTE3301-M209***, dans ses versions ***V1.00(ABLG.4)C0*** et antérieures.

2.8.5. Recommandations

Appliquer le correctif ***V1.00(ABLG.6)C0***. Celui-ci est disponible ici.

Des informations complémentaires sont disponibles sur le site du fabricant.

2.9. RCONFIG - CVE-2022-44384

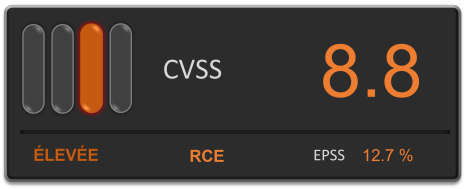

Figure 5. CVE-2022-44384

rConfig est un outil d'administration opensource permettant de réaliser périodiquement des *snaphsot* des configurations de périphériques réseau.

Un défaut de contrôle dans la fonction *PHP File Handler*, permet à un attaquant de téléverser des fichiers malveillants pour exécuter du code arbitraire sur le système

2.10. Informations

2.10.1. Risque

- Exécution de code arbitraire à distance.

2.10.2. Type de vulnérabilité

- **CWE-343**: Unrestricted Upload of File with Dangerous Type.

2.10.3. Criticité

Vecteur d'attaque : Réseau	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Fort
Complexité d'attaque : Faible	Portée : Inchangée	Impact sur la disponibilité : Fort
Privilèges requis : Faible	Impact sur la confidentialité : Fort	

2.10.4. Composants vulnérables

- rConfig version 3.9.6 et inférieure.

2.10.5. Recommandations

- Mettre à jour rConfig vers la version 3.9.7.
- Plus d'informations disponibles sur le github de l'utilitaire.

Un exploit (POC) est disponible en sources ouvertes.

3. Qakbot, une nouvelle campagne.

Le cheval de Troie Qakbot est actif depuis une dizaine d'années. Ciblant initialement le secteur bancaire, ce maliciel est largement employé lors de campagnes d'hameçonnages comme primo-infection, pour déployer ultérieurement d'autres implants malveillants.

Ce mois-ci, une nouvelle campagne exploitant une vulnérabilité Microsoft, permet d'installer cet info stealer en inhibant toute alerte de sécurité du dispositif *Mark of the Web*.

3.1. Mark of the web (MoTW)

La fonctionnalité *MoTW* permet de déterminer si un fichier provient d'internet par l'intermédiaire d'un *identifiant de zone*. Cet attribut est implémenté dans les propriétés du fichier.

```
Value  Setting
-----------------------------
0      My Computer
1      Local Intranet Zone
2      Trusted sites Zone
3      Internet Zone
4      Restricted Sites Zone
```

Figure 6. Valeurs possibles d'un identifiant de zone [Source: Microsoft].

Si cet identifiant a pour valeur "3", les applications prenant en charge l'attribut *MoTW* avertiront l'utilisateur, via une fenêtre de sécurité, de l'origine du fichier et exigeront une validation pour son ouverture ou exécution.

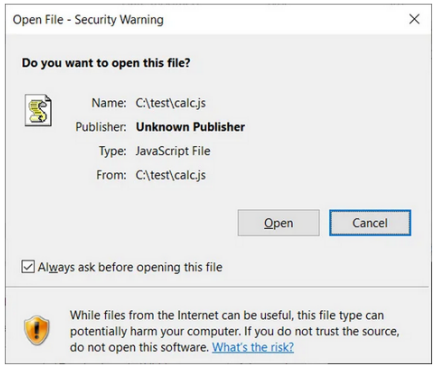

Figure 7. Exemple de fenêtre d'avertissement [Source: Bleepingcomputer].

3.2. Where is the MoTW ?

Lors de précédentes campagnes de phishing Qakbot, les attaquants procèdent au déploiement du maliciel via une archive, contenant un fichier *IMG*. Cette dernière renferme un raccourci windows *LNK* ainsi qu'une DLL nécessaire à son installation. Installation discrète, car le marquage *MoTW* n'est pas propagé au sein d'un fichier *IMG* ou *ISO*.

Cette vulnérabilité, identifiée avec la CVE-2022-41091, a été corrigée par Microsoft lors du Patch Tuesday de ce mois ci.

Toutefois, les attaquants emploient une nouvelle faille dans leur dernière campagne, inhibant le *MoTW*. Ce mode opératoire a été découvert par le chercheur en sécurité ProxyLife.

Cette nouvelle campagne d'hameçonnage délivre des courriels ne contenant pas de pièce jointe mais un lien

hébergeant une archive sécurisée, ainsi que le mot de passe pour l'ouvrir.

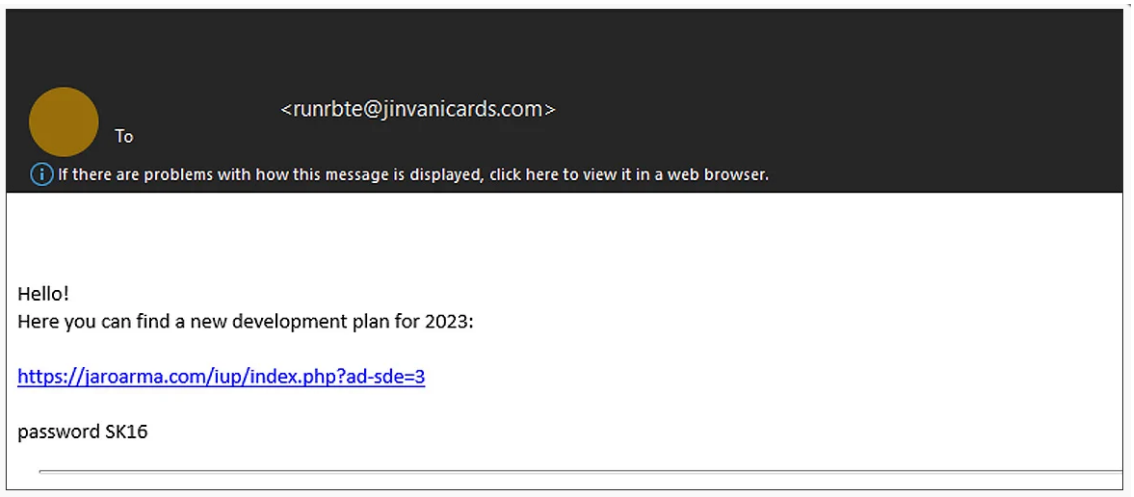

Figure 8. Exemple de courriel [Source: Bleepingcomputer].

La langue du corps du message est celle du pays visé.

La France a été ciblée par cette campagne.

Telles des *matriochkas*, cette archive renferme une nouvelle archive contenant un fichier *IMG*. Lors de son ouverture, un nouveau lecteur est monté sur le système d'exploitation proposant une arborescence. Cette arborescence liste un dossier ainsi que des fichiers dont un javascript.

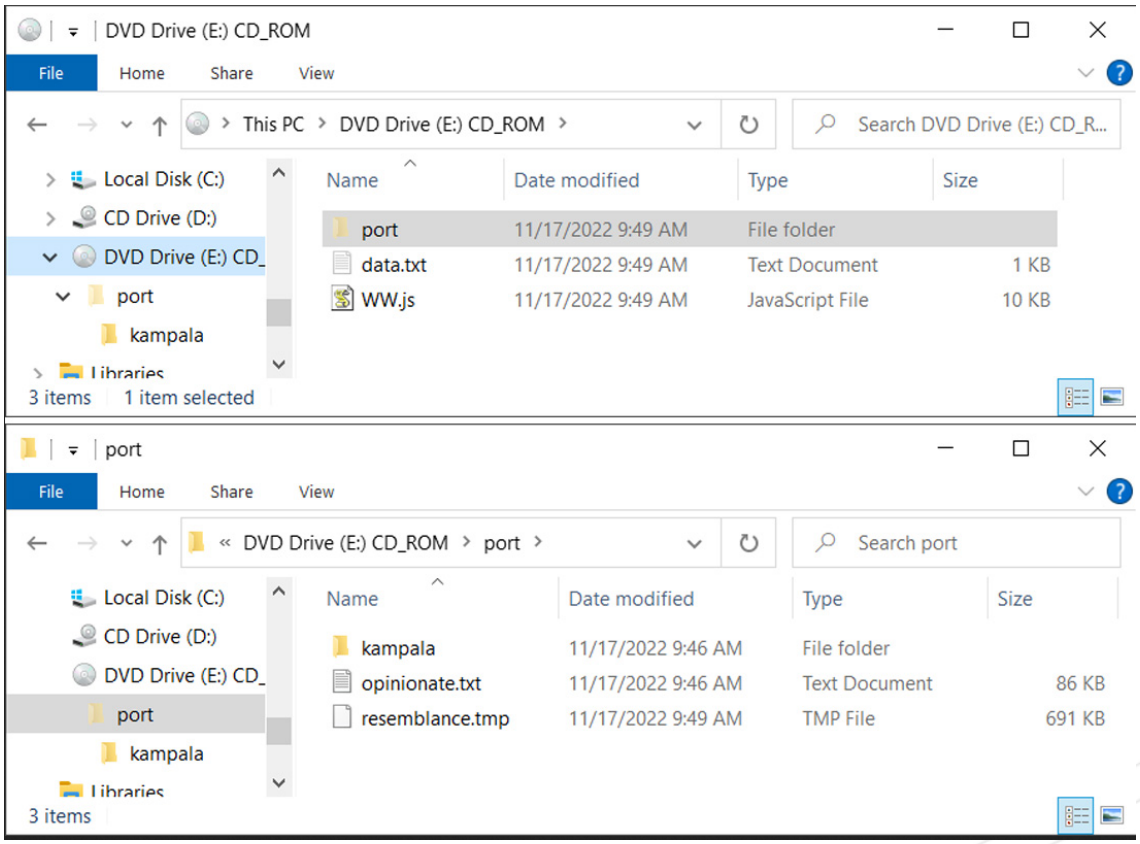

Figure 9. Contenu du lecteur montée [Source: Bleepingcomputer].

Depuis Windows 10, en double-cliquant sur un fichier IMG ou ISO, un nouveau lecteur est monté automatiquement.

Pour chaque campagne, les noms des fichiers et des dossiers sont différents.

Ce fichier *JS* embarque du code *VBScript* devant charger une librairie DLL, renommée en *.tmp* (dans le dossier *port*), via l'instruction regSvr32. Cette instruction est construite dynamiquement, en concaténant une chaîne de caractères présent dans le fichier et le contenu d'un autre fichier (*data.txt* pour cet exemple).

Malgré la provenance du fichier javascript, aucune fenêtre d'avertissement n'est initiée par Microsoft et le programme est exécuté.

L'attaquant exploite une faille en intégrant une signature malformée en base 64 dans le fichier, lui permettant de contourner l'attribution de l'identifiant de zone.

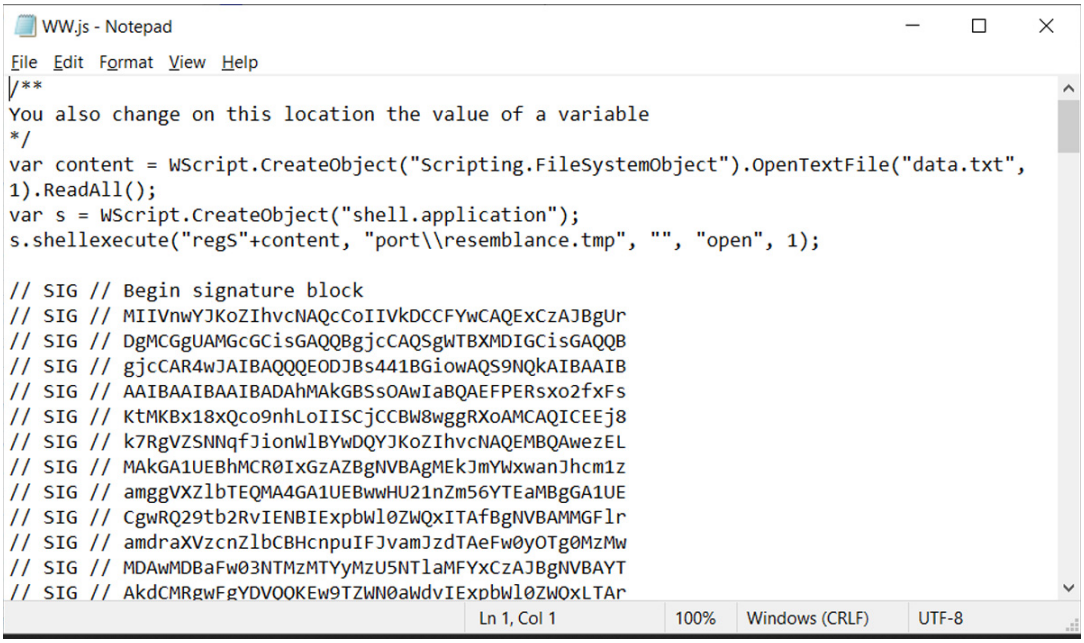

Figure 10. Fichier contenant du code VBScript et une signature malformée [Source: Bleepingcomputer].

Cette même signature malformée a été constatée lors de campagnes du ransomware Magniber menées en octobre.

Quelques minutes après l'enregistrement de la librairie, cette dernière est injectée dans un processus légitime (comme wermgr.exe et AtBroker.exe) pour éviter toute détection par les solutions de sécurité.

Microsoft a connaissance de cette vulnérabilité et de son exploitation par des groupes cybercriminels. Dans l'attente d'un correctif fourni par l'éditeur lors de son *Patch Tuesday*, le CERT aDvens recommande un renforcement de la sensibilisation des usagers sur les campagnes de phishing.

4. Hive

4.1. Portrait

Depuis sa découverte en juin 2021, à la suite de l'attaque de la principale organisation de santé californienne, le groupe cybercriminel Hive, spécialisé dans l'attaque par rançongiciel, semble avoir été particulièrement actif. En effet, selon des données publiées par le FBI en novembre 2022, le groupe aurait rançonné plus de 1300 organisations à travers le monde, amassant ainsi un butin de près de 100 millions de dollars.

Actuellement produit sous Rust, l'outil éponyme Hive est une variante de rançongiciel conçue pour être distribuée aux membres affiliés du groupe sous un modèle de Ransomware-as-a-service. Hive dispose de capacités lui permettant de cibler les systèmes Windows, Linux, VMware ESXi ou FreeBSD.

Dans l'objectif de fournir un service global aux membres affiliés, Hive dispose d'un portail API dédié permettant aux attaquants de centraliser la gestion de leurs attaques, le paiement des rançons, la publication sur le site de HiveLeaks etc. Toujours dans cette logique, Hive comprend également un service support et un service client.

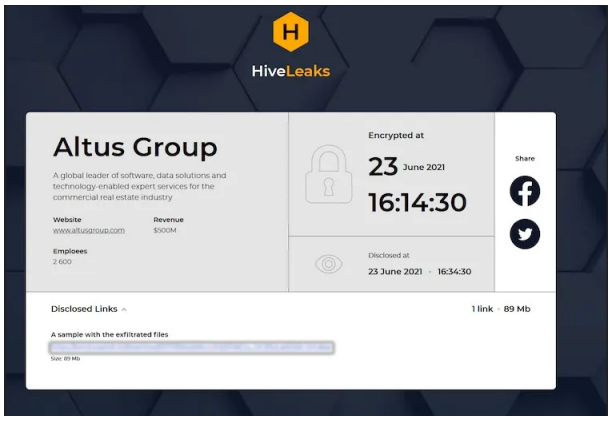

Figure 11. Publication du site de divulgation de données Hive Leaks

Les acteurs affiliés au groupe Hive, russophones pour la plupart, sont soupçonnés d'avoir appartenu au groupe Conti. Les membres de Hive sont également connus pour renouveler leurs attaques contre les victimes étant parvenues à récupérer leurs données sans avoir payé de rançon.

4.2. Cibles

Les campagnes menées par Hive indiquent que le groupe cybercriminel cible des secteurs diversifiés : des organisations gouvernementales à l'industrie lourde (Tata Power) en passant par des médias (Altice France) ou des centres de santé publics.

Ce dernier secteur est d'ailleurs une cible privilégiée du rançongiciel du fait de la difficulté à sécuriser les réseaux hospitaliers et la sensibilité des informations qui y transitent. Ainsi, peu de temps après son apparition, le groupe cybercriminel avait attaqué en août 2021 le centre hospitalier à but non lucratif *Memorial Health* en Ohio et Virginie-Occidentale. Quelques mois plus tard, en septembre 2021, Hive avait attaqué le *Missouri Delta Medical Center*, avec cette fois l'utilisation d'une tactique de double extorsion (chiffrement et menace de diffusion).

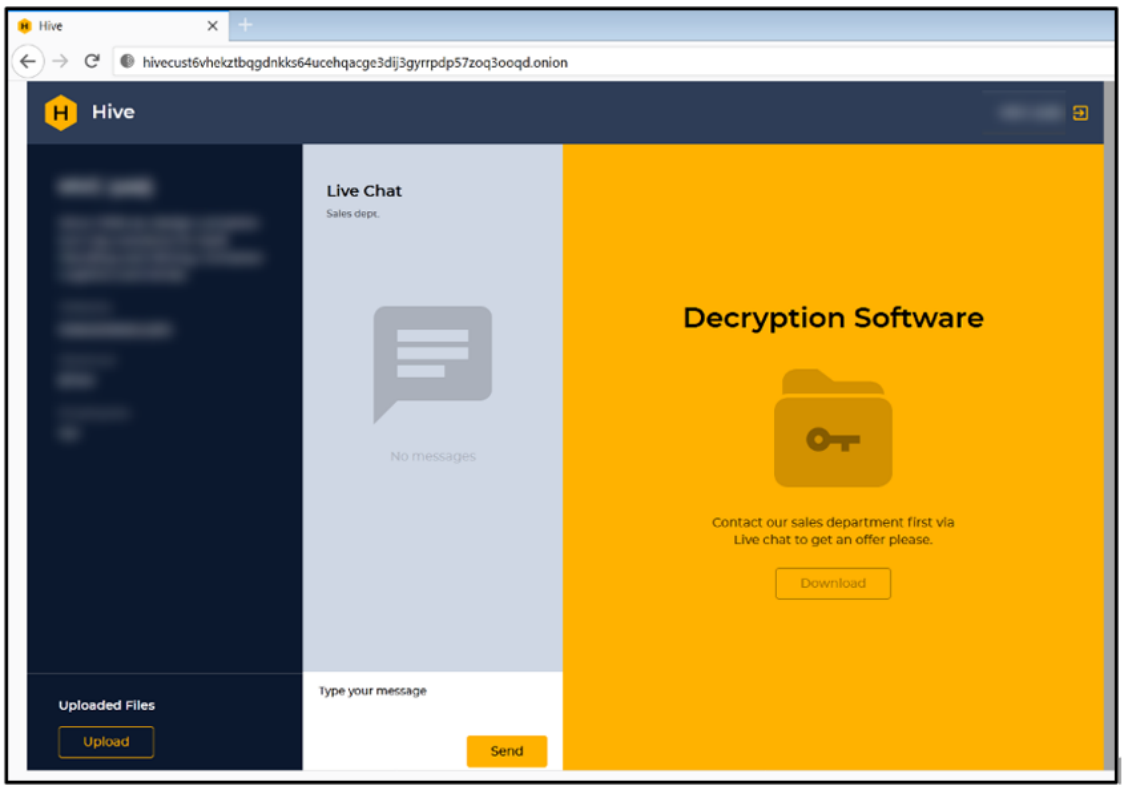

Figure 12. Portail de chat Hive destiné à la négociation et au paiement de la rançon.

4.3. Technique, tactique et procédure

4.3.1. Accès initial

L'attaquant utilise un large panel de techniques, s'adaptant au profil de la victime et profitant des opportunités se présentant à lui :

- campagnes d'hameçonnage,
- contournement des procédures d'accès via l'utilisation de protocoles de connexion à distance (VPN, RDP),
- exploitation de vulnérabilités telles que les CVE-2021-31207, CVE-2021-34473 et CVE-2021-34523,
- connexion à des serveurs FortiOS en contournant l'authentification multifacteur (MFA) via l'exploitation de la CVE-2020-12812.

4.3.2. Persistance

Pour garantir l'accès aux postes et serveurs compromis, Hive utilise : la création de tâches s'exécutant au redémarrage et l'affectation d'utilisateur (spécialement créé) aux groupes *Administrateurs* et *Utilisateurs du buerau à distance*.

4.3.3. Défense et évasion

Les attaquants du groupe Hive arrêtent les processus de sauvegarde et protection des fichiers, suppriment les sauvegardes existantes via *vssadmin* en ligne de commande ou via *PowerShell* et enfin, suppriment les journaux

d'événements Windows.

4.3.4. Exfiltration et Impact

Hive supprime les bases virales, désactive toutes les parties de Windows Defender et d'autres programmes antivirus dans le registre système. Le rançongiciel exfiltre ensuite les données ciblées à l'aide de l'outil *Rclone* et du service de stockage cloud *Mega.nz*. Les données sont ensuite chiffrées et un fichier nommé *.key** est déposé à la racine du système, nécessaire au déchiffrement, ce fichier n'existe que sur la machine où il a été créé et ne peut être reproduit.

Une note de rançon est créée dans chaque répertoire affecté. Celle-ci met en garde contre tout déplacement ou altération du fichier *.key** et invite les victimes à contacter le ***service commercial*** du groupe Hive via un portail de chat leur permettant de discuter du paiement de la rançon et du déchiffrement des fichiers.

Table 1. Matrice ATT&CK

Accès initial TA0001	Exécution TA0002	Évasion Défense TA0005	Exfiltration TA0010	Commandement et contrôle	Impact TA0040
Services à distance externes T1133	Interprète de commandes et de scripts T1059	Suppression de l'indicateur sur l'hôte T1070	Transférer des données vers un compte cloud T1537	Protocole de la couche application T1071	Chiffrement des données pour l'impact T1486
Exploiter l'application publique T1190	PowerShell T1059.001	Modifier le registre T1112		Protocoles Web T1071.001	Empêcher la récupération du système T1490
Hameçonnage T1566.001		Altérer les défenses T1562			

4.4. IoC

Le CISA, le FBI et le HHS ont publié en novembre 2022 un bulletin conjoint sur le rançongiciel Hive et ont mis à disposition du public des indicateurs de compromission. Le bulletin est disponible en références.

5. Références

Atlasian CVE-2022-43781

- https://nvd.nist.gov/vuln/detail/CVE-2022-43781
- https://www.cybersecurity-help.cz/vdb/SB2022111807
- https://jira.atlassian.com/browse/BSERV-13522
- https://cwe.mitre.org/data/definitions/78.html
- https://twitter.com/VietPetrus/status/1593858510806056960

Atlasian CVE-2022-43782

- https://nvd.nist.gov/vuln/detail/CVE-2022-43782
- https://www.cybersecurity-help.cz/vdb/SB2022111809
- https://jira.atlassian.com/browse/CWD-5888
- https://cwe.mitre.org/data/definitions/284.html
- https://cwe.mitre.org/data/definitions/287.html

Zyxel CVE-2022-40602

- https://nvd.nist.gov/vuln/detail/CVE-2022-40602
- https://www.cybersecurity-help.cz/vdb/SB2022112211
- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-pre-configured-password-vulnerability-of-lte3301-m209
- https://cwe.mitre.org/data/definitions/284.html
- https://cwe.mitre.org/data/definitions/287.html

D-Link CVE-2022-44808

- https://nvd.nist.gov/vuln/detail/CVE-2022-44808
- https://cve.report/CVE-2022-44808
- https://cwe.mitre.org/data/definitions/78.html

NetGear CVE-2022-44184

- https://nvd.nist.gov/vuln/detail/CVE-2022-44184
- https://exchange.xforce.ibmcloud.com/vulnerabilities/240595
- https://cwe.mitre.org/data/definitions/787.html

Article Qakbot

- https://www.bleepingcomputer.com/news/security/new-attacks-use-windows-security-bypass-zero-day-to-drop-malware/
- https://www.bleepingcomputer.com/news/security/qbot-phishing-abuses-windows-control-panel-exe-to-infect-devices/
- https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

Article Hive

- https://www.cisa.gov/uscert/ncas/alerts/aa22-321a
- https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/navigating-the-world-of-raas-a-dive-into-the-hive-ransomware-group-as-a-business/
- https://www.bleepingcomputer.com/news/security/fbi-hive-ransomware-extorted-100m-from-over-1-300-victims/

Article Cyberpsychologie (Définitions)

- https://www.universalis.fr/encyclopedie/abreaction/
- https://www.vulgaris-medical.com/encyclopedie-medicale/abreaction