TLP:WHITE

MENACES LIÉES AUX VOLS DE COOKIES ET CONTRE-MESURES

1.0

25 mai 2022

TLP:WHITE

Sommaire

1. Analyse de la menace

1.1. Une menace croissante

Les cookies [1] permettent de conserver des informations dans le navigateur pour une durée déterminée. De taille réduite (entre 0 et 4 kilo-octets), c'est un couple clé et valeur échangé entre le navigateur et le serveur lors de leurs communications au moyen des en-têtes HTTP « `Cookie` » (requête cliente) et « `Set-Cookie` » (réponse serveur). Ils sont idéals pour maintenir un état entre un serveur et son client. C'est pourquoi ils sont notamment utilisés pour maintenir ouverte la session d'un utilisateur initialement authentifié après avoir fourni son mot de passe. Le déploiement de solutions d'authentification unique (*SSO*), et l'utilisation de consoles d'administration dans le navigateur web font peser une menace croissante sur l'usage des cookies de session.

Les cookies permettant d'authentifier un utilisateur deviennent une cible privilégiée car ils peuvent permettre à un attaquant de se substituer à la connaissance d'un couple identifiant et mot de passe pour usurper l'identité d'un utilisateur [2]. Ils peuvent être utilisés comme vecteur initial de compromission, mais également comme un moyen de latéralisation, particulièrement vers des ressources hébergées dans le *cloud*.

Les cookies sont régulièrement collectés par des acteurs cybercriminels avec l'aide des *stealer* [1] déposés sur les systèmes de leurs victimes ou lors d'opération d'hameçonnage [2]. Ces informations d'authentification peuvent être directement réutilisées pour accéder aux comptes utilisateur des victimes, ou revendues sur des places de marchés spécialisées telles que Genesis, Russian Market, ou encore Black Hat Forum [4]. L'achat d'identifiants et de cookies de session permet d'accéder à des systèmes et applications en ligne, tels que les VPN (*virtual private network*), les VDI (*virtual desktop infrastructure*) ou des gestionnaires d'identités comme Azure Active Directory ou Okta.

Ces cookies sont également convoités par les attaquants, car ils permettent de contourner la plupart des solutions d'authentification multifacteurs, puisque les sessions dérobées sont déjà authentifiées [3]. Enfin, ils peuvent être visés dans le cadre de compromissions ciblées, lorsqu'un attaquant est présent sur le système d'informations de sa victime, et qu'il souhaite se latéraliser vers un environnement *cloud*, ou simplement lorsque l'organisation utilise un système d'authentification unique dans le navigateur web pour accéder à ses ressources (comme Office365).

1.2. Un levier pour l'écosystème cybercriminel, l'exemple du groupe LAPSUS$

En mars 2022, la compromission de la société Okta par le groupe LAPSUS$ a fait la une de nombreux journaux spécialisés. La société Okta est spécialisée dans la gestion d'identités et d'accès et sa compromission peut impliquer un risque pour une partie de ses clients parmi lesquels de nombreuses grandes entreprises [5]. Cet incident notable a été plus médiatisé que la compromission d'Electronic Arts (EA) en juin 2021 par le groupe LAPSUS$, ou à minima l'un de ses membres. Pour la compromission, un cookie de session a été employé comme vecteur d'intrusion [6], [7].

L'achat d'un cookie de session pour 10 $ aurait permis à l'attaquant de se connecter au Slack d'EA, et de demander des jetons au support technique de l'entreprise afin de contourner l'authentification à facteurs multiples pour se connecter au réseau d'EA. Le code source du jeu FIFA 2021, du moteur de jeu Frostbite ainsi que d'autres outils internes auraient été exfiltrés par le groupe d'attaquants pour un total d'environ 780 Go de données [8, 9].

1. On peut citer par exemple les codes **Qakbot**, **CryptBot**, **AZORult** ou encore **Vidar Stealer** [3, 4].
2. Les proxies **evilginx2** ou **muraena** sont par exemple utilisés pour collecter des cookies à la volée.

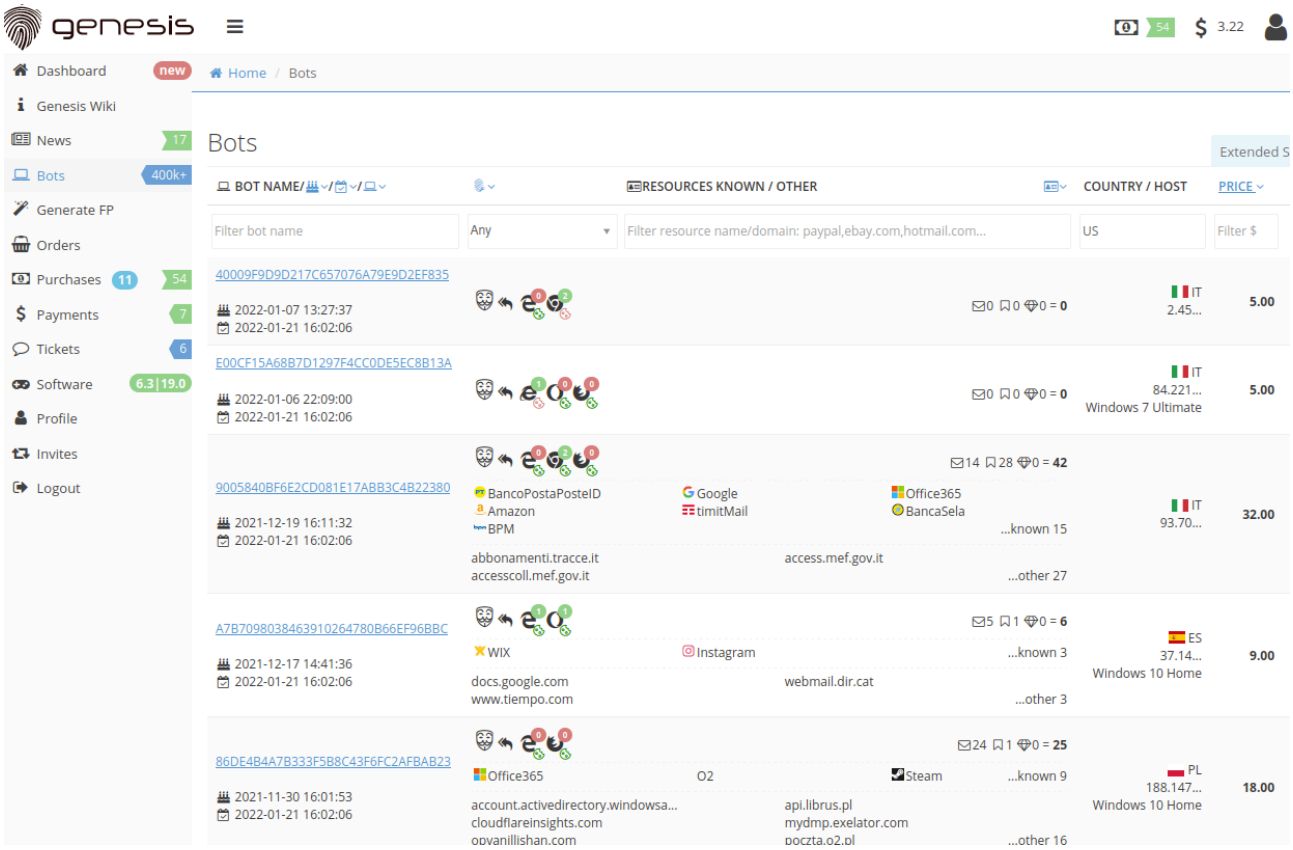

Fig. 1.1. – Capture d'écran de la place de marché spécialisée Genesis, sur laquelle un attaquant peut acheter des cookies volés permettant de s'authentifier sur un site internet [10].

1.3. Usage par des modes opératoires stratégiques, l'exemple de NOBELIUM

Des acteurs stratégiques s'intéressent également aux cookies de session lors de leurs campagnes d'intrusion. Selon plusieurs éditeurs de solution de sécurité, le mode opératoire NOBELIUM associé à la compromission de SolarWinds en 2020 aurait notamment eu recours au vol de cookies de session à plusieurs reprises.

- Au cours de l'années 2020, Volexity a investigué plusieurs incidents visant un think tank et employant le mode opératoire DARK HALO, que l'entreprise associe à NOBELIUM. Lors de l'un d'entre eux, l'attaquant a dérobé une clé privée associée à l'outil Duo. Cette dernière lui a permis de générer des cookies de session « `duo-sid` » valides pour accéder à une application Microsoft Outlook déléguant l'authentification multifacteurs à la solution Duo MFA [11].
- Fin 2021, l'éditeur Mandiant, qui suit le mode opératoire sous l'appellation UNC2452, a observé l'attaquant accéder à l'environnement Microsoft 365 d'une organisation en utilisant un cookie de session volé. Mandiant a découvert que certains postes de travail de la victime avaient été infectés par le *stealer* **CryptBot** peu de temps avant la génération du cookie. L'éditeur émet l'hypothèse que l'attaquant se soit procuré le cookie auprès des opérateurs de **CryptBot**. Mandiant a également observé que l'attaquant s'est latéralisé sur un hyperviseur VMWare en utilisant le cookie de session d'un compte privilégié [12].
- Début 2022, l'éditeur CrowdStrike a mis à jour ses observations sur la campagne StellarParticle qu'il associe à la compromission de SolarWinds. L'attaquant a réussi à contourner l'authentification multifacteurs pour accéder à un compte privilégié Office365 grâce à la récupération des cookies du navigateur Chrome. Pour ce faire, il a réalisé une élévation de privilège sur le poste d'un administrateur qui avait passé un challenge multifacteurs récemment. Une fois en possession des fichiers du navigateur, il a déchiffré les cookies en utilisant une clé DPAPI. Les cookies ont ensuite été ajoutés à une nouvelle session à l'aide de l'extension Chrome Cookie Editor que l'attaquant a installée sur un serveur compromis et supprimée après utilisation [13].

2. Recommandations

2.1. Politique de sécurité associée aux sessions authentifiées

Durée de vie et révocation des sessions

Afin de réduire la durée d'utilisation d'une session volée par un attaquant, il est recommandé d'en limiter la durée de validité. Par exemple, la durée d'une session d'authentification pour accéder à des informations sensibles ou à des privilèges élevés doit être très réduite (quelques minutes tout au plus).

Cette recommandation doit être particulièrement prise en compte lors de l'utilisation de session sans état [3] (*stateless*) car la révocation d'un cookie peut s'avérer particulièrement complexe.

Il est en outre possible de durcir le mécanisme de session par diverses mesures :

- pour les opérations sensibles, exiger une réauthentification ;
- mettre en place des mesures de détection d'usurpation de session [4] ;
- journaliser les actions associées à une session ;
- dans le cas d'une authentification mutuelle, vérifier à chaque requête qu'un identifiant de session est toujours associé au même certificat client.

Ces options ne sont malheureusement pas toujours configurables, et en particulier pour les services *cloud* (*Software as a Service*, *SaaS*). La granularité du paramétrage des sessions est un facteur à prendre en compte dans le choix des solutions d'authentification, en adéquation avec les objectifs de sécurité du système d'information. En l'absence de contrôle sur les paramètres des sessions, les informations échangées sur un service externe, telle qu'une messagerie instantannée, doivent être maîtrisées car l'authenticité des utilisateurs n'est pas fiable.

Par exemple l'application web Slack, vraisemblablement utilisée pour usurper l'identité d'un salarié lors de la compromission de l'entreprise Electronic Arts en juin 2021 [8], ne propose pas de définir un délai d'expiration de session en dehors des offres payantes [a]. Une fois authentifié, un utilisateur peut ainsi rester connecté indéfiniment - rendant le vol de session d'autant plus risqué, puisque celle-ci sera valide pendant plusieurs mois après sa création.

a. D'après la documentation de Slack, seule l'offre « Enterprise » permet de déployer une politique d'expiration des sessions alors que pour les offres « Pro » et « Business » le délai de validité n'est pas propagé aux sessions existantes : `https://slack.com/help/articles/115005223763-Manage-session-duration-` (consultée le 30 mars 2022).

Mots de passe et authentification multifacteurs

Si l'authentification multifacteurs (aussi connu sous les termes anglais de *MFA* ou *2FA* lorsque deux facteurs sont nécessaires) est une mesure efficace pour réduire les conséquences d'une compromission de mot de passe, elle ne permet pas de se prémunir contre le vol de jeton de session. L'ensemble de nos recommandations sur le déploiement de l'authentification multifacteur est disponible dans le guide ANSSI « *Recommandations relatives à l'authentification multifacteur et aux mots de passe* » diffusé en octobre 2021 [5].

3. Dans le cas d'une session sans état, le cookie se suffit à lui même, et ne dépend pas d'une session stockée côté serveur. Cette approche est notamment utilisée par le standard JSON Web Tokens (JWT) où le cookie est signé cryptographiquement et vérifié par le serveur à chaque requête.

4. Par exemple, si l'adresse IP et les horaires de connexion d'un client sont incohérents, on peut exiger une nouvelle authentification, au moins pour les opérations les plus sensibles.

5. Recommandation R12 du guide relatif à l'authentification multifacteur et aux mots de passe [14].

Développement de services web authentifiés

Pour les concepteurs de services web utilisant des sessions authentifiées, des recommandations concernant la bonne gestion des cookies sont présentes dans la section 5.5 du guide « *Recommandations pour la mise en oeuvre d'un site Web : maîtriser les standards de sécurité côté navigateur* » [6].

Gestion des droits utilisateurs

La gestion des sessions doit bien entendu se doubler d'une bonne gestion des droits selon les bonnes pratiques habituelles : comptes nominatifs, vérification systématique des autorisations lors d'un accès à une ressource protégée, respect du principe du moindre privilège, gestion formalisée du cycle de vie des comptes, journalisation des accès, etc. Pour ce faire, il est possible de se référer au « *Guide d'hygiène informatique* » de l'agence [15].

2.2. Durcissement du système d'information d'administration

Les attaques par vol de session sont d'autant plus dévastatrices lorsque celles-ci atteignent la couche d'administration d'un système d'information, offrant des privilèges élevés à un attaquant. Ainsi, il est recommandé d'utiliser des postes dédiés à l'administration sans les exposer aux usages bureautiques, à la navigation web ou à des messageries. De manière générale, plus un système possède de privilèges, plus ses usages doivent être restreints afin d'en limiter la surface d'attaque. Ceci permet d'élever le niveau sécurité des systèmes d'information d'administration sachant qu'ils représentent des cibles prioritaires pour les attaquants.

Pour répondre aux multiples besoins des administrateurs, plusieurs architectures de cloisonnement sont recommandés, par niveau de sécurité décroissant au regard des objectifs de sécurité fixés :

- un poste d'administration dédié ;
- un poste d'administration multi-niveaux ;
- un poste d'administration avec accès distant à un système d'information bureautique ;

Ces solutions, et leurs possibles implémentations, sont décrites en détail dans la section 4.2 du guide « *Recommandations relatives à l'administration sécurisée des systèmes d'information* » [16].

6. Recommandations R26 à R33 du guide relatif à la mise en oeuvre d'un site web [2].

A. Annexe

A.1. Techniques, Tactiques et Procédures issues de la matrice ATT&CK

TTP	Nom	Description
T1539	Steal Web Session Cookie	An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has succesfully authenticated to a website.
T1550.004	Use Alternate Authentication Material : Web Session Cookie	Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.
T1606.001	Forge Web Credentials : Web Cookies	Adversaries may forge web cookies that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies to authenticate and authorize user access.

B. Bibliographie

[1] IETF. *RFC 6265, HTTP State Management Mechanism, Domain matching*. 1er mai 2011.
URL : https://datatracker.ietf.org/doc/html/rfc6265.

[2] ANSSI. *Guide ANSSI-PA-009 : Recommandations pour la mise en oeuvre d'un site Web : maîtriser les standards de sécurité côté navigateur.* 28 avril 2021.
URL : https://www.ssi.gouv.fr/guide/recommandations-pour-la-securisation-des-sites-web/.

[3] INTRINSEC. *Analysis of LAPSUS$ Intrusion Set*. 28 mars 2022.
URL : https://www.intrinsec.com/threat-intel-report/.

[4] MICROSOFT. *DEV-0537 Criminal Actor Targeting Organizations for Data Exfiltration and Destruction*. 22 mars 2022.
URL : https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/.

[5] SEKOIA.IO. *Lapsus$: When Kiddies Play in the Big League*. 23 mars 2022.
URL : https://www.sekoia.io/en/lapsus-when-kiddies-play-in-the-big-league/.

[6] Brian KREBS. *A Closer Look at the LAPSUS$ Data Extortion Group*. 23 mars 2022.
URL : https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/.

[7] UNIT42. *Threat Brief : Lapsus$ Group*. 24 mars 2022.
URL : https://unit42.paloaltonetworks.com/lapsus-group/.

[8] VICE. « How Hackers Used Slack to Break into EA Games ». 11 juin 2021.
URL : https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack.

[9] VICE. « Inside the Market for Cookies That Lets Hackers Pretend to Be You ». 16 juin 2021.
URL : https://www.vice.com/en/article/n7b3jm/genesis-market-buy-cookies-slack.

[10] KREBSONSECURITY. *Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code*. 22 avril 2022.
URL : https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/.

[11] VOLEXITY. *Dark Halo Leverages SolarWinds Compromise to Breach Organizations*. 14 décembre 2020.
URL : https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/.

[12] MANDIANT. *Suspected Russian Activity Targeting Government and Business Entities Around the Globe*. 6 décembre 2021.
URL : https://www.mandiant.com/resources/russian-targeting-gov-business.

[13] CROWDSTRIKE. *Early Bird Catches the Wormhole : Observations from the StellarParticle Campaign*. 27 janvier 2022.
URL : https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/.

[14] ANSSI. *Guide ANSSI-PG-078 : Recommandations relatives à l'authentification multifacteur et aux mots de passe.* 10 août 2021.
URL : https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/.

[15] ANSSI. *Guide d'hygiène informatique*. 1er septembre 2017.
URL : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/.

[16] ANSSI. *Guide ANSSI-PA-022 : Recommandations relatives à l'administration sécurisée des systèmes d'information*. 11 mai 2021.
URL : https://www.ssi.gouv.fr/administration/guide/securiser-ladministration-des-systemes-dinformation/.

1.0 - 25 mai 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN