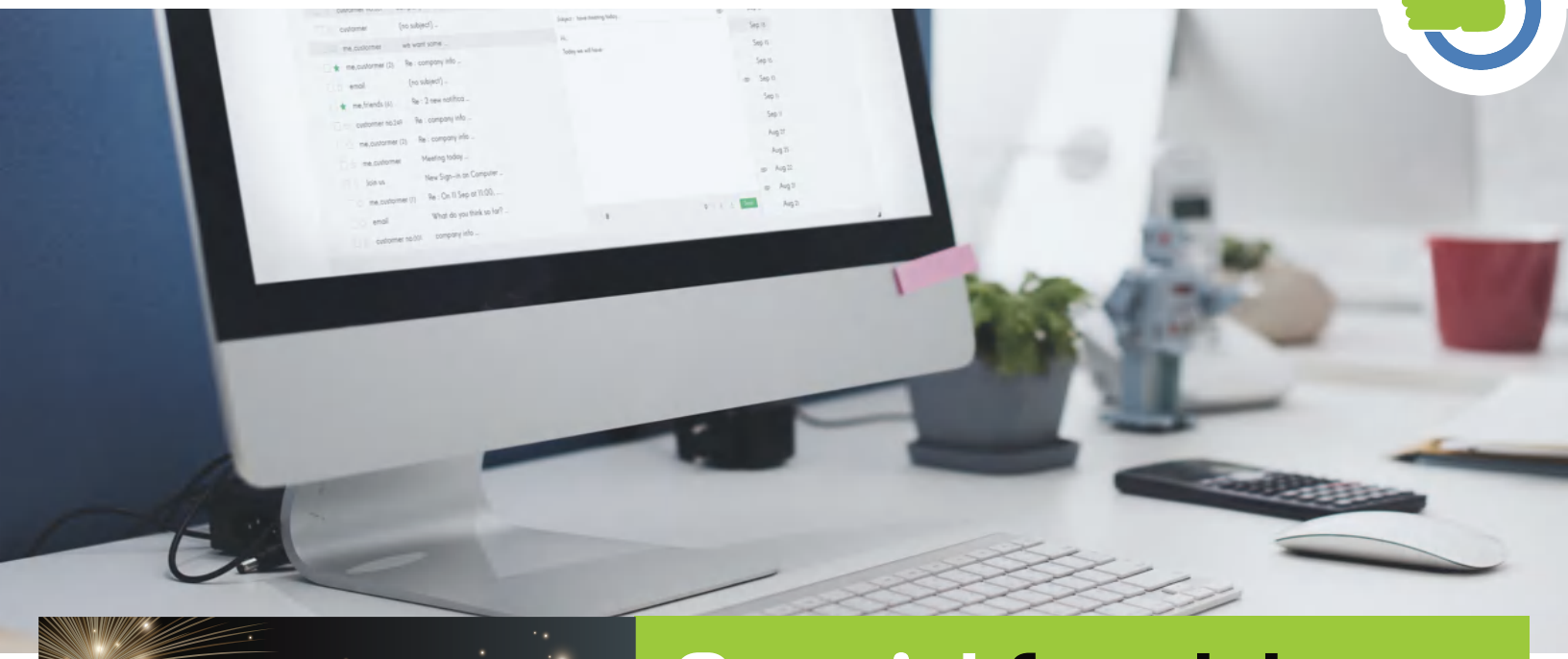
Janvier 2022 • Vol. 9 n° 1

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies

Entreprise TI classée #1 à Québec en 2021 par **ThreeBest Rated®**



2022 BONNE ANNÉE

à tous nos clients et partenaires!

Merci d'être là pour nous depuis toutes ces années et de nous permettre de faire la différence en contribuant à votre succès d'affaires.

Toute l'équipe d'ARS Solutions vous souhaite une bonne et heureuse année couronnée de succès!

Que cette nouvelle année soit pour vous riche en projets et moments inspirants. Qu'elle soit également une opportunité de dépassement de soi et de fierté.

Courriel frauduleux ingénieux

Tout comme votre entreprise, vos fournisseurs peuvent être la cible des cybercriminels et voir leur réseau infecté à la suite d'une tentative d'hameçonnage fructueuse.

Le mois dernier, chez ARS Solutions, nous avons reçu un courriel à l'adresse générale de l'entreprise (info@ars-solutions.ca) et celui-ci semblait très légitime. Il provenait du traiteur avec qui nous avions fait affaire pour notre dernier 5 à 7 corporatif d'Halloween.

Le courriel contenait la véritable bannière de signature professionnelle de notre personne-ressource avec qui nous avions planifié le buffet et il faisait mention d'un virement bancaire qui avait été effectué suite à l'événement.

SUITE PAGE 2

Pour consulter le virement en question, **nous devions cliquer sur un lien qui menait vers une page de connexion à un compte Microsoft pour accéder au fichier via OneDrive.** Certains employés ne se sont pas sentis concernés par ce courriel et l'ont tout simplement ignoré, mais ceux qui avaient organisé le 5 à 7 corporatif ou qui s'occupaient de la comptabilité ont cliqué.

C'est au moment d'entrer les identifiants personnels (adresse courriel et mot de passe) que certains des employés visés ont réalisé que quelque chose clochait. Nous avons rapidement communiqué avec notre personne-ressource qui travaillait au traiteur en question pour valider que cet envoi provenait bien d'elle, qui nous a confirmé le contraire. **On s'est donc empressé de contacter les employés concernés pour vérifier leur réaction et si leur ordinateur avait été infecté d'une quelconque façon.**

Dans ce cas-ci, il ne s'agissait que d'une tentative d'hameçonnage pour usurper les identifiants de nos employés et personne n'a entré ces informations, mais **le simple fait de cliquer sur le lien aurait pu être bien dommageable pour notre entreprise et infecter l'ensemble du réseau.**

En cybersécurité, un seul clic peut être fatal. On doit se méfier d'absolument tout pour éviter le pire, car il vaut mieux être paranoïaque que piraté… N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet ou pour vérifier la légitimité d'un courriel reçu.

info@ars-solutions.ca - 418-872-4744 #233

ALERTE CONCOURS!

Pour célébrer l'arrivée de la nouvelle année, ARS Solutions aimerait vous gâter. C'est pourquoi nous avons décidé de faire tirer une carte ***Visa prépayée de 250 $*** parmi tous les abonnés de notre chaîne YouTube ***le lundi 31 janvier prochain à 10h00***. L'annonce du ou de la gagnant(e) se fera sur notre page Facebook le jour du tirage.

Pour participer, vous n'avez qu'à rechercher ***ARS Solutions*** sur YouTube pour accéder à notre chaîne et vous y abonner. Faites vite, vous avez jusqu'au lundi 31 janvier 2022 à 10h00 pour participer!

info@ars-solutions.ca - 418-872-4744 #233

La faille Log4J se transforme en pandémie avec plus de 840 000 attaques en 72 heures

Le 14 décembre, des chercheurs en sécurité ont révélé que des cybercriminels avaient utilisé la faille Log4J récemment découverte dans plus de 840 000 cyberattaques. On estime que cette faille est présente dans **plus de 100 millions d'applications/sites Web dans le monde. Son niveau de criticité est maintenant de 10/10.** Il s'agit de la faille de sécurité la plus importante vécue jusqu'à présent. Elle peut affecter l'ensemble des systèmes informatiques présentement. Si bien que la recommandation du Center for Internet Security (CIS) est de **demeurer extrêmement vigilant en effectuant une cybersurveillance constante afin d'être en mesure de détecter tout comportement anormal des systèmes et d'intervenir sur-le-champ.**

Lorsque la vulnérabilité initiale a été rendue publique, elle a été décrite comme un jour zéro (ou 0day), ce qui signifie qu'elle a été potentiellement exploitée avant que les développeurs de logiciels n'en connaissent l'existence. La société de sécurité Check Point a surveillé la situation de près et elle a constaté plus de 100 attaques Log4J par minute.

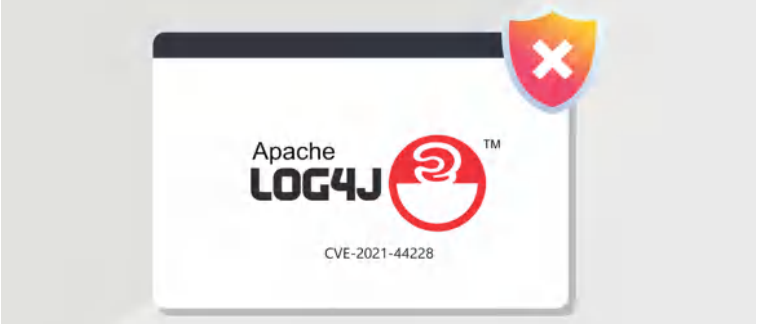
Le 14 décembre, les chercheurs ont découvert que la correction développée était incomplète et le fournisseur, Apache, en a publié une nouvelle. Le 17 décembre, deux nouveaux problèmes ont été confirmés et le jour suivant, Apache a publié un autre correctif. **Nous nous attendons à ce que ce cycle de corrections de vulnérabilités se poursuive, car les attaquants et les chercheurs continuent de se concentrer sur Log4J.**

Vous devez corriger cette faille en priorité

En raison de la large étendue de Log4J et des preuves que **les acteurs malveillants ciblent activement les entreprises disposant de versions vulnérables de Log4J,** le CIS encourage toutes les organisations à **faire de la correction de cette grave vulnérabilité leur priorité absolue.** Il est important de noter que la simple mise à jour de Log4J peut ne pas résoudre les problèmes. La mise à jour vers la version la plus récente d'un logiciel ne supprimera pas les accès obtenus par les malfaiteurs. Le CIS recommande de **faire preuve de vigilance en enquêtant sur l'activité dans votre environnement,** en recherchant des preuves d'accès non autorisés et en agissant conformément aux meilleures pratiques de réponse aux incidents pour en réduire l'exposition.

L'une des plus graves vulnérabilités jamais vues

« Cette vulnérabilité est l'une des plus graves que j'ai vues dans toute ma carrière, si ce n'est la plus grave », a déclaré Jen Easterly, directrice de l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA). Elle a ajouté que la faille pourrait avoir un **impact sur des centaines de millions d'appareils. Check Point a noté que les cybercriminels exploitant Log4J l'utilisaient pour prendre le contrôle d'ordinateurs afin d'effectuer toutes sortes d'opérations,** du minage de cryptomonnaies à l'envoi de spam en passant par le lancement d'attaques DDoS avec de grands botnets. **Les malfaiteurs ont ciblé des entreprises du monde entier,** y compris des acteurs de premier plan comme Apple, Amazon, IBM, Microsoft et Cisco.



L'utilisation du logiciel est devenue une pandémie à part entière. Une faille dans Java est utilisée pour lancer des attaques par exécution de code à distance qui **peuvent prendre le contrôle total d'un système.** « Avec cette vulnérabilité, les attaquants obtiennent **un pouvoir presque illimité - ils peuvent extraire des données sensibles, télécharger des fichiers sur le serveur, supprimer des données, installer des rançongiciels et plus encore »**, a déclaré Nicholas Sciberras, responsable de l'ingénierie chez Acunetix.

Voici ce que nous vous recommandons :

1. Lister toutes vos applications Web/sites Web publiés sur Internet;

2. Fermer le(s) site(s) jusqu'à ce que les vérifications de vulnérabilités requises soient faites :

a. Consulter votre équipe informatique interne, votre fournisseur Web externe ou demander l'aide de votre partenaire TI afin qu'ils procèdent aux vérifications.
b. Obtenir les correctifs et les appliquer.

3. Remettre vos applications en ligne.

Les entreprises ne doivent pas sous-estimer la gravité de la situation. Celles qui effectuent déjà une cybersurveillance de leurs systèmes sont mieux préparées pour y faire face. **Une vigilance accrue dans la surveillance de vos réseaux** pour détecter les comportements anormaux est nécessaire pour appliquer des actions de réponse immédiate.

Si vous avez besoin de plus d'informations, n'hésitez pas à communiquer avec notre équipe de support à dispatch@ars-solutions.ca ou par téléphone au (418) 872-4744, poste 1.

Source : Cal Jeffrey et Center for Internet Security (CIS)

Microsoft va mettre finalement fin à Internet Explorer en 2022

Internet Explorer ne sera plus pris en charge à partir de juin 2022

Si vos employés ont encore l'habitude d'utiliser Internet Explorer, sachez qu'ils devront changer de navigateur sous peu. Microsoft mettra définitivement fin à Internet Explorer l'année prochaine, après plus de 25 ans. Le navigateur Web désuet a été largement inutilisé par la plupart des consommateurs pendant des années, mais **Microsoft va mettre officiellement le dernier clou dans le cercueil d'Internet Explorer le 15 juin 2022,** en le retirant au profit de Microsoft Edge.

« Nous annonçons que **l'avenir d'Internet Explorer sur Windows 10 est dans Microsoft Edge** », déclare Sean Lyndersay, un responsable du programme Microsoft Edge. « L'application de bureau Internet Explorer 11 sera retirée et ne sera plus prise en charge le 15 juin 2022, pour certaines versions de Windows 10. »

Windows 10 comprendra encore Internet Explorer cette année, mais toutes les versions grand public mettront fin au support du navigateur. Microsoft ne le dit pas clairement, mais il est probable que nous verrons finalement la fin d'Internet Explorer intégré à Windows en juin 2022 ou peu après.

L'alternative pour la plupart des entreprises sera Microsoft Edge avec le mode IE qui prend en charge les anciens contrôles ActiveX, qui sont étonnamment toujours utilisés par de nombreuses entreprises. Les contrôles ActiveX sont la version des modules d'extension d'Internet Explorer. Par exemple, le lecteur Flash d'Internet Explorer est un contrôle ActiveX. Malheureusement, **les contrôles ActiveX ont été une source importante de problèmes de sécurité.** Ils pourraient surveiller vos habitudes de navigation personnelles, installer des logiciels malveillants, générer des fenêtres contextuelles, enregistrer vos frappes au clavier et vos mots de passe et faire d'autres choses malveillantes. **Microsoft va tout de même continuer de prendre en charge ce mode IE dans Edge jusqu'en 2029 au minimum.**

La fin d'Internet Explorer est attendue depuis longtemps. L'année dernière, Microsoft a mis fin à la prise en charge d'Internet Explorer 11 pour l'application Web Microsoft Teams et prévoyait même l'interdire pour l'accès aux services de Microsoft 365. **Depuis le 17 août dernier, Internet Explorer 11 n'est plus pris en charge pour les services en ligne de Microsoft tels qu'Office 365, OneDrive, Outlook, etc.**

Microsoft a également essayé d'empêcher les gens d'utiliser Internet Explorer depuis plus de 5 ans. Microsoft Edge est apparu pour la première fois en 2015, et il a donné le coup d'envoi de la fin de la marque Internet Explorer. Depuis, **Microsoft a qualifié Internet Explorer de "solution de compatibilité" plutôt que de navigateur et a encouragé les entreprises à ne plus utiliser le navigateur obsolète au profit d'Edge et de son mode IE.**

Source : Tom Warren et AZURPLUS

ARSolutions
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744