PODRIM Magazine

NUMERO 20

Dec - Jan - Fev - 2022 | N°020 (Digital Edition) | FREE on Web | www.PODRIM.com

Digital édition

Decembre
Janvier
Février

www.PODRIM.COM

SOMMAIRE

Vous tenez dans votre main le Numéro20 du Magazine de votre association préférée.
Oui, le Numéro19 n'est jamais paru, cela est normal car il ne contenait que des informations sur des évènements, news et soirées que malheureusement les confinements dues à la pandémie ont annulés ou perturbés.

Alors, 2022, nouvelle année, un nouvel espoir (référence, hin !).
Le 12 JANVIER 2022 nous vous retrouveront une dernière fois pour fêter les 10 ans de la RetroAnimé au Mange Disque avant d'aller vers de nouveaux projets.
Après presque 50 soirées, nous avions fait le tour de la question. Mais nous ferons d'autres soirées rétro et nostalgiques.

Nous vous proposons dans ce numéro un article faisant le tour des films, séries ou gammes de jouets ayant utilisé le Slime comme accessoire, ou comme personnage principal et ils sont nombreux.
Vous en rappelez vous de tous ?
A tout les copain(e)s et Ourson(ne)s, je vous souhaite le meilleur pour 2022.

BIENTOT
AU
CINEMA

Ressortez votre Gameboy et sa GameboyCam

Il y a plus de deux ans, on évoquait dans les colonnes de Presse-citron **la petite console portable Analogue Pocket**. Une petite console portable fortement inspirée de la Game Boy Pocket de Nintendo côté look, avec toutefois des fonctions très "*modernes*", et la possibilité de lire les jeux Game Boy, Game Boy Color et Game Boy Advance. Mieux encore, via des adaptateurs, elle peut lire les cartouches SEGA Game Gear, Neo Geo Pocket Color et Lynx. La bonne nouvelle, c'est que cette Analogue Pocket est désormais disponible à la commande.

Alors évidemment, comme c'est le cas pour à peu près tout ce qui touche le secteur du jeu vidéo depuis plus d'un maintenant, n'espérez pas passer commande et recevoir votre Analogue Pocket dans les prochains jours. En effet, la petite console (dont le tarif a été gonflé à 219,99 dollars) ne sera pas livrée avant plusieurs semaines... voire plusieurs mois. Les concepteurs vont catégoriser les acheteurs en trois groupes, et il se peut ainsi que votre commande passée à l'instant ne vous soit livrée... qu'en 2023 !

CONCOURS

le plus beau PULL de NOEL

Cette année nous avons organisé un concours du plus beau Pull de Noel.

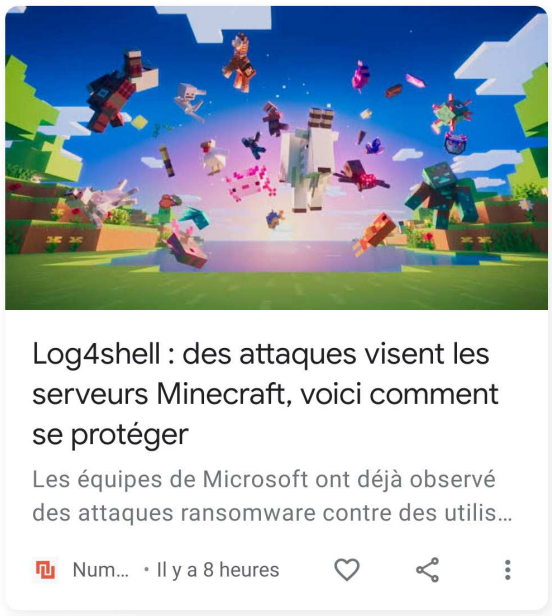
Retrouvez les photos de tout les participants sur le site de PODRIM PODRIM.com

Le GAGNANT est indiscutablement Obywan avzec son Pull GREMLINS Très drôle.

WIN

«Log4Shell»

la faille de sécurité décrite comme le plus grand piratage de l’histoire d’Internet



Les piratages massifs de données sont devenus si courants que nous sommes insensibles aux attaques, piratages et autres exploits 0-day. Mais cette nouvelle attaque 0-day, baptisée Log4Shell, est si importante qu'elle est déjà considérée comme le pire piratage Internet de l'histoire.

Vous ne savez pas encore de quoi il s’agit, mais le hack « Log4Shell » permet déjà à de nombreux hackers d’accéder aux systèmes informatiques et aux serveurs de très nombreuses entreprises. Les experts ont déjà vu Log4Shell pour la première fois en action dans le jeu Minecraft. Ce qui est fou avec ce hack, c’est que seulement quelques lignes de texte transmises dans un chat peuvent suffire pour pénétrer les défenses d’un ordinateur cible.

Cette faille a été décrite publiquement vendredi 10 décembre 2021 (le CERT-FR dans ce bulletin) et se trouve dans la bibliothèque de journalisation Apache log4j. Elle a été analysée comme critique avec note de 10/10 pour sa dangerosité. Ce qui est visé par l’attaque est un outil qui permet l’enregistrement des informations relatives à un logiciel, comme les rapports d’erreurs ou n’importe quel log.

Plus concrètement, on peut facilement envoyer du code à cet outil qui va le lire sur le serveur cible. Ce qui permet d’installer des outils d’accès à distance sur les réseaux des victimes. On s’attend donc à de nombreuses attaques de ransomware dans les jours, semaines et mois à venir.

En plus du correctif, les équipes de sécurité informatique du monde entier doivent procéder à une évaluation approfondie de l’activité du réseau pour détecter et supprimer toute trace d’intrus.

Théoriquement, tout le monde peut être touché par cette faille. Log4j est omniprésent dans quasiment tous les serveurs utilisant Java. Apple iCloud, Tesla, Steam, Twitter ou encore Cloudflare pourraient avoir été touchés. Le Québec, par exemple, a décidé de surprendre l’accès à ses 4000 sites et services gouvernementaux.

C’est une vulnérabilité très grave en raison de l’utilisation très répandue de Java, il est impossible d’estimer l’impact sur cette vulnérabilité.

Des comptes cloud Google sont piratés pour miner des cryptomonnaies

Le dernier rapport des équipes de cybersécurité de Google sur leur Cloud évoque une écrasante majorité de services piratés utilisés pour miner des cryptomonnaies.

Dans un rapport publié fin novembre par les services de cybersécurité de Google, le géant américain dresse un tableau des menaces informatiques qui visent sa plateforme cloud. Parmi les utilisation faites des instances piratées, un phénomène se détache particulièrement : le minage de cryptomonnaies.

Le chiffre est écrasant. 86% des instances compromises du Cloud Google ont été utilisées pour miner des crypto. Concrètement, les pirates volent votre puissance de calcul pour obtenir des fragments de bitcoin ou d'ether à vos frais. Ce chiffre est très nettement devant les 10 % de cas où le cloud est utilisé pour scanner d'autres cibles, une pratique qui permet aux pirates de trouver des serveurs ou des appareils vulnérables en balayant internet. Des systèmes sans protection, avec des ports ouverts par exemples, qui permettraient aux attaquant de s'introduire dans les systèmes facilement, pour voler des donner ou lancer un rançongiciel.

Enfin, 8 % des instances piratées sont utilisées pour lancer directement des attaques. Les attaques Ddos, ou attaques par déni de services, sont par exemple lancées à l'aide d'un grand nombre de machines piratées pour saturer un site internet. Le total dépasse 100 % car certaines instances hackées ont été utilisées de plusieurs manières.

Les équipes de Google ont également identifié les vulnérabilités exploitées pour ces attaques. Fait tristement habituel, les faibles mots de passe et l'absence d'identifiants sont responsables dans quasiment la moitié des cas. 48 % exactement. L'occasion de rappeler qu'il est primordial d'avoir des mots de passe compliqués, (minimum 8-10 caractères, majuscules, caractères spéciaux) et différents pour chaque compte, en utilisant au besoin un gestionnaire de mots de passe.

Les principales autres catégories de vulnérabilités sont les failles dans des logiciels tiers ou directement des services Cloud de Google (26%) et la mauvaise configuration de ces services (12% des cas).

Google arrête Glupteba, un botnet constitué d'un million de machines

Un large réseau d'ordinateurs infectés par un logiciel maleillant, utilisé notamment pour mener des attaques par rançongiciel, a été mis hors service par Google, qui porte plainte contre deux Russes suspectés d'être aux commandes du botnet.

Un botnet utilisé notamment pour mener des attaques par rançongiciel est la cible d'une action judiciaire de la part de Google. Le 7 décembre, Google a annoncé la mise hors d'état de nuire de Glupteba, un réseau d'un million d'appareils infectés par ce cheval de Troie, fonctionnant sous Windows et utilisant la blockchain pour se protéger. L'entreprise de Mountain View précise qu'il s'agit de la première action en justice contre ce type de botnet.

Glupteba infecte les machines par le biais de publicités malveillantes (diffusées notamment sur le réseau Google Ads) qui déclenchent le téléchargement du malware si l'utilisateur clique dessus, et de programmes d'affiliation Pay per install. A partir de là, le malware peut voler des données contenues dans le navigateur web de la victime, puis les utiliser dans le but de pirater des comptes, effectuer des achats frauduleux, infecter d'autres machines, revendre les données, déclencher des attaques par rançongiciel ou par déni de service, etc. Les ordinateurs infectés, mis en réseau et contrôlés par les cybercriminels, sont également utilisés pour le minage de cryptomonnaies.

Selon Google, le botnet Glupteba se réplique en infectant un millier de nouvelles machines par jour, dans le monde entier.

Google indique dans un communiqué avoir réussi à mettre ce botnet hors de contrôle des pirates, grâce à l'aide de partenaires (hébergeurs, plateformes cloud). Mais l'entreprise précise qu'un mécanisme de backup utilisant la blockchain Bitcoin le rend plus résilient, autrement dit il y a un risque de le voir redémarrer, à l'image de ce qui s'est passé pour Emotet.

La plainte, déposée à New York pour – entre autres – fraude et violation de propriété intellectuelle, vise deux opérateurs du botnet suspectés de résider en Russie, Dmitry Starovikov et Alexander Filippov.

Des milliards de smartphones et PC connectés en WiFi et Bluetooth comportent une grave faille de sécurité

Mauvaise nouvelle, toutes les puces connectées en WiFi et Bluetooth sont victimes d’une grave faille de sécurité. En insérant du code dans le processeur, les chercheurs ont été capables de supprimer toutes les données et d’exécuter des programmes malveillants. La vulnérabilité a depuis été corrigée chez plusieurs constructeurs.

Aujourd’hui, la grande majorité de nos appareils sont connectés à un réseau WiFi. Certains ajoutent même le Bluetooth pour encore plus de versatilité, ce qui rend bien souvent notre quotidien plus facile. Mais ces protocoles qui se sont imposés dans nos vies ne sont pas sans faille. Des chercheurs en cybersécurité de l’université de Darmstadt apportent une nouvelle preuve dans un rapport qui détaille la vulnérabilité qu’ils ont découverte.

Bien qu’ils contiennent pour la plupart des composants WiFi, Bluetooth et LTE séparés, nos appareils connectés se partagent bien souvent les mêmes ressources, comme une antenne, à titre d’exemple. Ce sont ces ressources que les chercheurs ont exploité pour découvrir la faille. En effet, elles permettent de lancer diverses attaques qui, à leur tour, permettent d’obtenir différents privilèges au sein des puces.

Les chercheurs ont ainsi découvert un total de neuf vulnérabilités. Bonne nouvelle, certaines peuvent être corrigées par une simple mise à jour du firmware. Les constructeurs concernés, à savoir Broadcom, Silicon Labs et Cypress, ont été prévenus et ont d’ores et déjà déployé un correctif sur leur processeur. Notons par ailleurs qu’Intel, Qualcomm ou encore AMD ne font pas partie de la liste, ce qui doit bien arranger ce dernier déjà victime d’une grosse faille de sécurité en septembre.

La mauvaise nouvelle, c’est que certaines vulnérabilités ne peuvent être réglées que par une refonte totale de la puce. Autrement dit, ce sont encore des millions d’appareils qui sont toujours impactés par les failles. D’autant que ces dernières permettent au pirate l’ayant exploité d’exécuter du code malveillant, voire de supprimer la totalité des données stockées. Pour se protéger d’une éventuelle attaque, les chercheurs conseillent de se déconnecter des appareils Bluetooth et réseaux WiFi inutiles.

L'Anssi réagit à la faille de sécurité Log4Shell

Vu ailleurs L'Anssi, par la voix de son directeur général Guillaume Poupard, ne s'est pas montrée aussi alarmiste que certains experts par rapport à la faille de sécurité Log4Shell. Bien qu'elle soit qualifiée de "grave", les choses devraient doucement rentrer dans l'ordre. "Dans un mois, on n'en parlera probablement plus, ça sera résiduel", a-t-il confié.

Guillaume Poupard, le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), a qualifié de "grave" la faille informatique baptisée "Log4Shell" révélée il y a quelques jours.

Il s'agit d'une vulnérabilité dans la bibliothèque open source de journalisation Log4j, développée par Apache. Elle touche un nombre de victimes potentielles très important puisque cette bibliothèque est très souvent utilisée dans les projets de développement Java/J2EE ainsi que par les éditeurs de solutions logicielles sur étagère basées sur Java/J2EE.

Cette faille "promet des fêtes de fin d'année un peu pénibles pour beaucoup d'experts", a ajouté le directeur général, sollicité à l'occasion d'une conférence de presse à propos du futur campus consacré à la cybersécurité à la Défense le 14 décembre et cité par Le Monde. Il s'est également montré rassurant : "dans un mois, on n'en parlera probablement plus, ça sera résiduel". Un discours beaucoup moins alarmiste que celui tenu par certains experts qui qualifient Log4Shell de la plus grande vulnérabilité informatique de l'histoire.

Il reste désormais à savoir si mais surtout comment cette vulnérabilité peut être exploitée pour mener des attaques. En pratique, elle permet une exécution de code arbitraire sur un serveur vulnérable par un attaquant sans qu'il n'ait besoin de s'authentifier. Sur ce sujet, Guillaume Poupard s'est montré plutôt inquiet : "j'ai peur qu'en creusant (...) on se rende compte de conséquences qui peuvent être relativement graves". La principale crainte est que la faille ait été exploitée "depuis beaucoup plus longtemps qu'on ne l'imagine".

C'est l'équipe de sécurité d'Alibaba Cloud qui aurait découvert en premier cette faille et prévenu Apache, d'après les informations de Bleeping Computer. Il est donc fortement recommandé d'utiliser la version la plus récente (2.15.0) le plus rapidement possible pour éviter d'être pris pour cible par un acteur malveillant. Mais pour certains, ce n'est pas suffisant, à l'image de Québec qui a ordonné le dimanche 12 décembre la fermeture préventive de l’ensemble de ses systèmes informatiques accessibles depuis l’Internet, soit 3992 sites et services.

EXPO CINE

Ghostbusters
EXO1
La voiture culte à Paris (au BHV)

Pour fêter la sortie de SOS.Fantôme 3 avec le casting original, les producteurs ont envoyé en exposition sur Paris une des voitures ayant servis sur le tournage.
Un rêve de gosse d'avoir pu la voir, comme la Doloréan de Retour vers le Futur, Kitt (K2000) ou Choupette (la Coccinelle).

MUSCLOR (jouets)

DOSSIER SLIME (les origines)

MUSCLOR (HE-MAN) est la première série à utiliser le Slime comme accessoire des jouets (alors qu'il n'est pas présent dans la série animée.

Ghostbusters (jouets)

DOSSIER SLIME
(les origines)

Ghostbusters (SOS.Fantôme), est la seconde gamme de joeuts à utiliser le Slime. Mais là il est présent dans les films et les séries animées, de par une logique scientique que le contacte entre humain et spectre provoque l'apparition du fameux Slime.
Il sera de couleur verte tout comme dans MUSCLOR.

Ninja Turtles (jouets)

DOSSIER SLIME
(les origines)

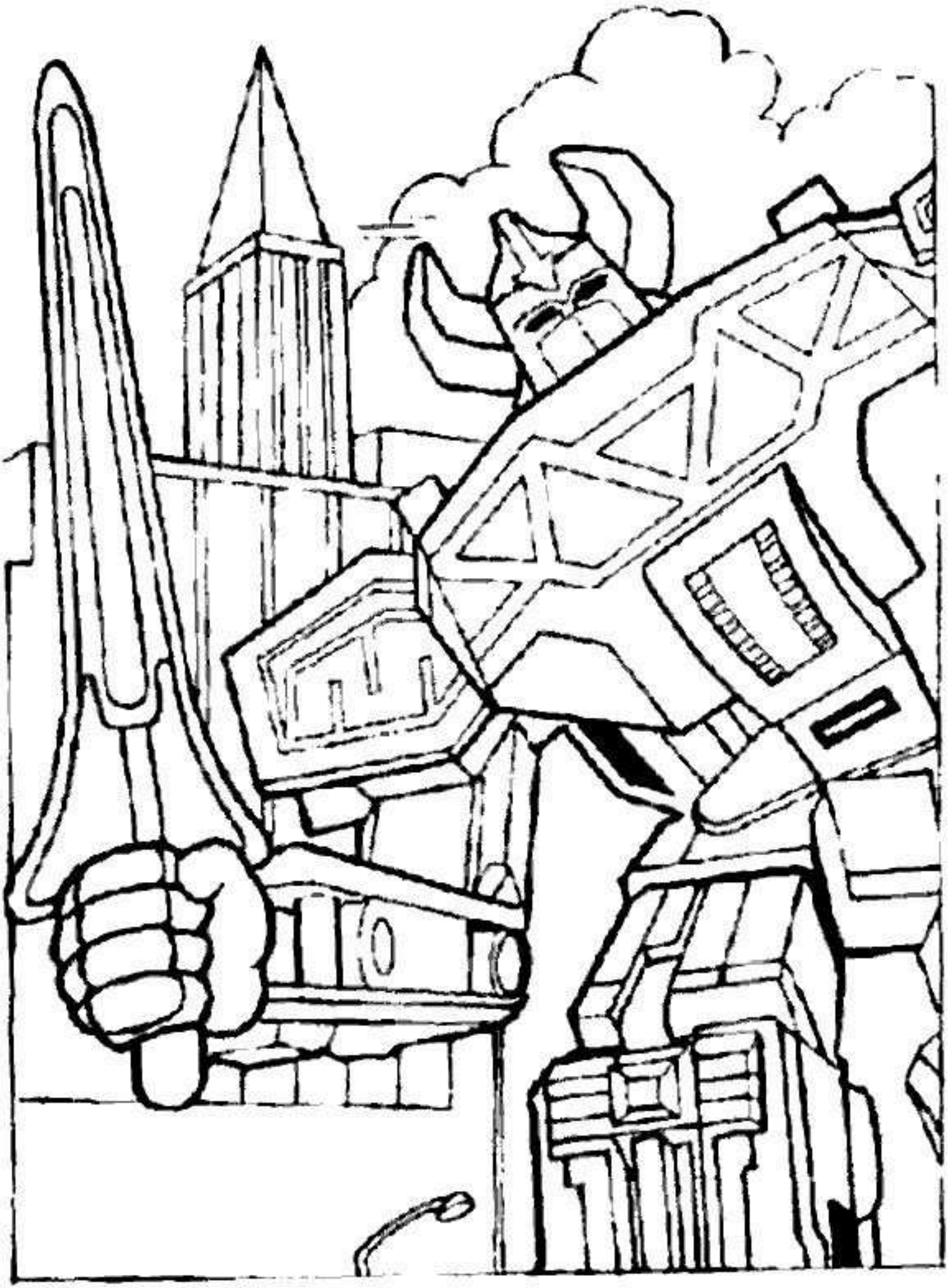
Dans les TORTUES NINJA, là encore le Slime (appellé ici Mutagène), encore de couleur verte, et partie intégrante du scénario des BD, films et séries, est utilisé comme dans SOS Fantôme et Musclor. Même composition, même couleur.

SOS Fantôme étaient encore en cours de diffusion et du coup pour se différencier lancera son Slime de couleur violette.

POWER RANGERS (série)

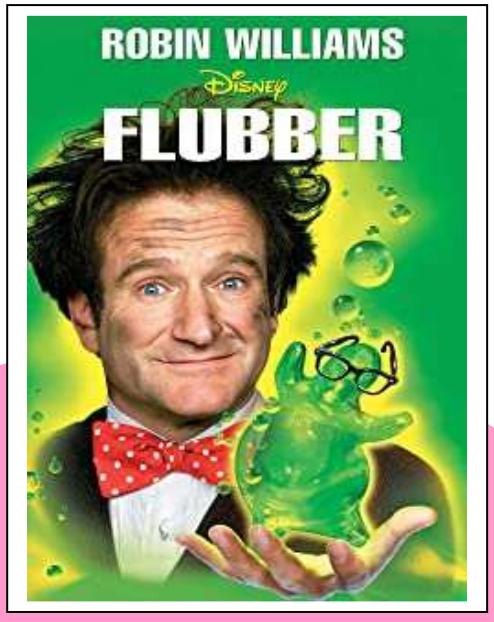
DOSSIER SLIME (les origines)

Pour son film au Cinéma Américain avec costumes et monstres originaux (non issus des séries japonaise comme à la TV), un ennemi est créé utilisant le OOZE (nom donné au Slime du film) pour aspirer l'énergie des humains.
Là encore il fait partis du scénario.



FLUBBER (film)

DOSSIER SLIME
(les origines)



Face aux succès dans les salles obscures des Tortues Ninja, Ghostbusters et des Power Rangers, Disney (le roi des produits dérivés) se met en tête d'avoir son propre film utilisant le Slime.

Dans le scénario, un gentil scientifique découvre une matière gélatineuse vivante qui peu servir à fabriquer pleins d'objets comme de la pâte à modelé mais également source d'énergie.
Le Film sera un flop tout comme les produits dérivés.

Les CRADOS (stickers)

DOSSIER SLIME
(les origines)

Fin des années 90, la série des CRADOS est relancé en Europe avec un troisième album, ainsi qu'une série animé diffusée sur Canal+ Malheureusement l'échec de l'album et la diffusion confidentielle de la série font que le Slime n'en sera pas distribués en France.

Les pays de l'est (Allemagne en tête) ainsi que latino (Italie et Espagne) vont avoir des pots de Slime contenant de petites figurines surprise, prémices des jouets «Pate à Prout» et autre figurines poubelles.

Docteur MAD (jeu)

DOSSIER SLIME (les origines)

Nickelodeon (chaine tv)

Jeu de plateau ou l'on crée des monstres, pleins de Slime entre les organes, pour les disséquer.

Le Slime a été pendant plus de 10ans la marque de fabrique comique de la chaîne pour enfants.

Silly Putty (gadget)

Silly Putty à l'origine créé pour trouver une alternative au caoutchou très chère après la 2nd guerre.
Jugé trop mou, il sera transformé à gadget pour les enfants.

Licorne Poo (jouets)

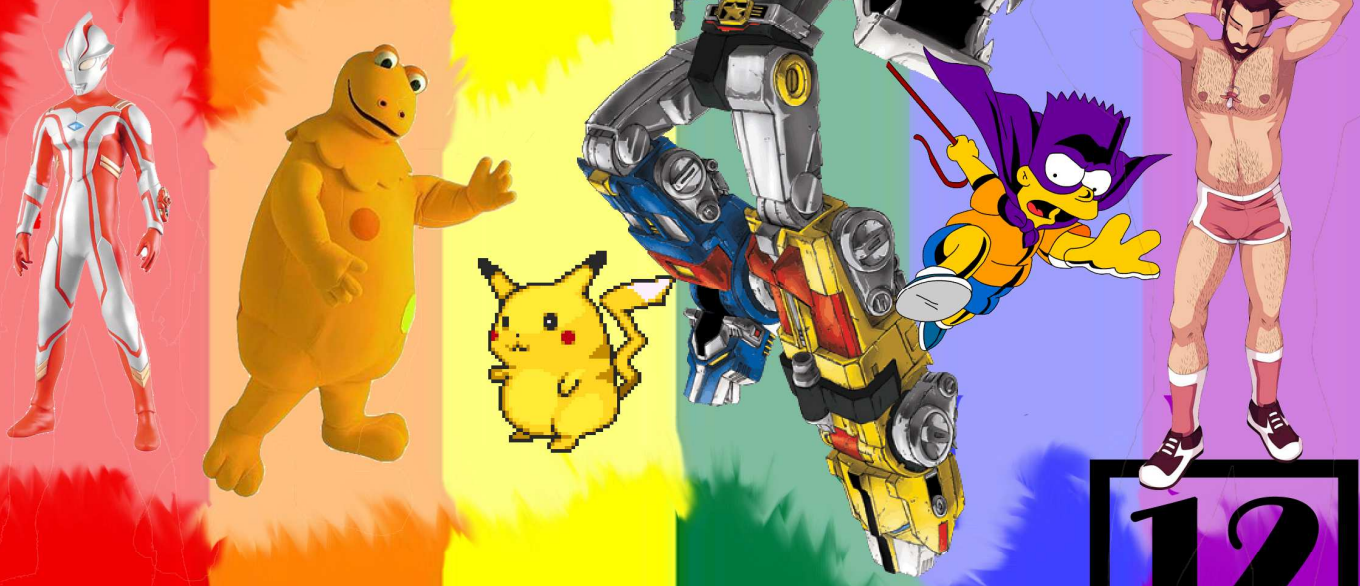
Maintenant le Slime est de toutes les couleurs avec des paillettes à l'esprit Licornes et Princesses.

UN ÉVÈNEMENT PODRIM CONCEPT

RETRO ANIME

LAST LEVEL

FREE ENTREE



12 Jan 2021

dès 19h00

12 JANVIER 2022

JOYEUX ANNIVERSAIRE 10Ans

APERO - AMBIANCE MUSICALE
CADEAUX - QUIZZ
EXPOSITION SURPRISE

UNE PRODUCTION PODRIM.COM AVEC au Mange-Disque EN PARTENARIAT AVEC Télé 80

au Mange Disque 15 Rue de La Reynie 75004 Paris

www.PODRIM.com