Veille technologique

Le sujet de ma veille comporte sur les principales attaques et failles matériels ou logiciels.

Les outils

- Pour cette veille technologique j'utiliserai un script python que j'ai coder qui va me permettre de récupérer les flux RSS de différents sites notamment ceux de l'ANSSI et les mettre dans un fichier que je pourrai filtrer comme je veux.

- J'utiliserai aussi l'application feedly sur mon téléphone que je consulterai régulièrement et je piocherai les articles qui se rapproche le plus de mon thème

```
import feedparser
import os
from datetime import datetime
flux = ['https://www.ssi.gouv.fr/feed/actualite/','https://korben.info/feed','https://www.ssi.gouv.fr/feed/publication/','https://www.lemondeinformatique.fr/flux-rss/thematique/toutes-les-actualites/
for url in flux:

#url ="https://korben.info/feed"
    file = open(r'fluxrss.txt', 'a+')
    file.write("********************************************************************************************** \n \n \n")
    file.write("La source RSS :  " + url + "  La date :  " + str(datetime.now()))
    file.write("\n")

    feed= feedparser.parse(url)
    for entry in feed.entries:
        title = entry.title
#        print(title)
        #publication = entry.published
        #print(publication)
        link = entry.link
#        print(link)
        #summary = entry.summary
        #print(summary)
        #content = entry.content
        #print(content)

        file.write(entry.title + "  ")
        file.write(entry.link)
        #file.write(entry.published)
        #file.write(entry.summary)
        #file.write(str(entry.content))
        file.write("\n")
        file.write("\n")
        file.write("\n")

    file.close()
cmd = 'mv fluxrss.txt /flux/$(date -I).txt'
os.system(cmd)
cmd = 'bash envoieFluxMail.sh'
os.system(cmd)
```

Cette veille technologique sera essentiellement accès sur la sécurité informatique.

Nous sommes au début du mois de janvier 2022.

LOG4J

Le 16 décembre une vulnérabilité qui touche les serveurs apache2 est trouvée il est possible d'injecter du code javascript qui peut être malveillant grâce aux logs le code qui sera lu par le serveur ne sera pas rendu inoffensif mais sera interprété et pourra faire télécharger et exécuter un logiciel malveillant au serveur

https://datavalue-consulting.com/faille-apache-log4j/#:~:text=Quelle%20est%20l'%C3%A9tendue%20de,d%C3%A9pendants%20du%20code%20log4j%20affect%C3%A9

https://www.ssi.gouv.fr/publication/lanssi-alerte-sur-la-faille-de-securite-log4shell/

18/01

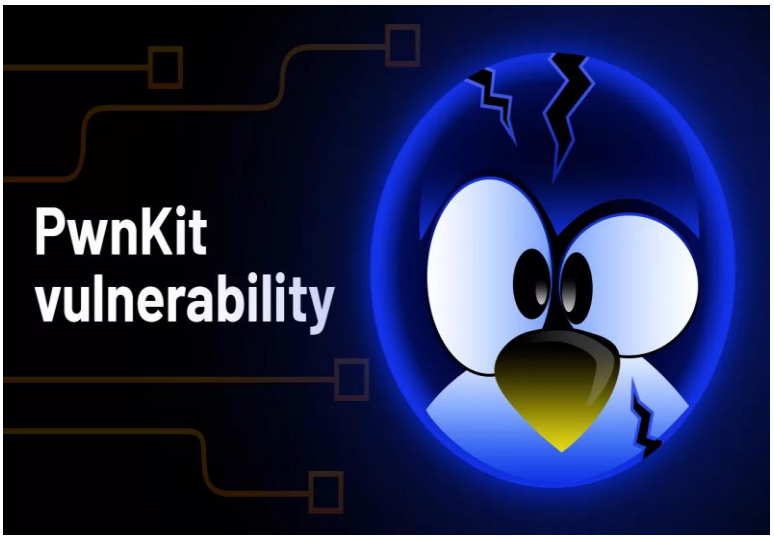
LE GANG REVIL MIS HORS D'ÉTAT DE NUIRE, PEUT-ÊTRE

L'etat Russe Ont Arrete 14 Membres De Ce Hroype De Hackers Spécialisé Dans Le Ransomware

Https://Cert.Ssi.Gouv.Fr/Avis/Certfr-2022-Avi-066/?Fbclid=Iwar11kiafaq0bm-Qyceh7qywa5ocgn4n1qz_Eiisat1w-Zwetgak3oe1hmhe

Ce gang été particulièrement connu pour ses ransonmware qui ont été devastateur.

25/01



Enorme faille de sécurité sur linux qui existe depuis 10 ans

PwnKit, le bug Linux qui permet d'obtenir un accès root à n'importe quelle machine fonctionnant sous linux, c'était un bug lié à un framework qui gère les interactions des processus avec privilèges ou non.

https://korben.info/pwnkit-exploit.html

Les conflits international augmentent le risque de failles de sécurité et d'attaque

La tension entre la Russie et l'Ukraine c'est aussi sur la plan cybersecurité

Telex : Google Maps limité en Ukraine et Russie, Le co-inventeur d'Ethernet est mort, Fitbit rappelle 1,7 million de montres connectées

https://www.lemondeinformatique.fr/actualites/lire-telex-google-maps-limite-en-ukraine-et-russie-le-co-inventeur-d-ethernet-est-mort-fitbit-rappelle-1-7-million-de-montres-connectees-86002.html

L'Ukraine aurait obtenu des informations personnelles sur environ 120 000 soldats russes engagés dans le conflit, notamment des noms, des adresses, des numéros de passeport, etc.

http://securite.developpez.com/actu/331555/L-Ukraine-aurait-obtenu-des-informations-personnelles-sur-environ-120-000-soldats-russes-engages-dans-le-conflit-notamment-des-noms-des-adresses-des-numeros-de-passeport-etc/

Microsoft identifie et atténue de nouveau malware ciblant l'Ukraine « en 3 heures », une opération qui aurait duré des semaines voire des mois il y a quelques années, selon le VP de la sécurité

http://securite.developpez.com/actu/331541/Microsoft-identifie-et-attenue-de-nouveaux-malware-ciblant-l-Ukraine-en-3-heures-une-operation-qui-aurait-dure-des-semaines-voire-des-mois-il-y-a-quelques-annees-selon-le-VP-de-la-securite/

Des hackers ont piraté des organismes de recherche spatiale russes

https://www.01net.com/actualites/des-hackers-ont-pirate-des-organismes-de-recherche-spatiale-russes-2055332.html

Guerre en Ukraine : des malwares, probablement d'origine russe, sabotent des ordinateurs

https://www.01net.com/actualites/guerre-en-ukraine-des-malwares-probablement-d-origine-russe-sabotent-des-ordinateurs-2055016.html

On peut voir que les données à caractère personnelle font parler d'elles dans tous les sujets sur des conflits international entre comme la guerre en Ukraine il y'a beaucoup de risques de vols ou destruction de données à caractère personnelles appartenant aux entreprises.

Des failles et attaque dans des organisme publique et privée (libre ou pas)

Ici on peut voir que même les lycées ne sont pas épargnés par les cyber-attaques, même des fabricants de carte graphique comme Nvidia

L'ENT des lycées franciliens touché par une cyberattaque (MAJ)

https://www.lemondeinformatique.fr/actualites/lire-l-ent-des-lycees-franciliens-touche-par-une-cyberattaque-maj-85995.html

Nvidia confirme être compromis à la suite d'une cyberattaque

https://www.lemondeinformatique.fr/actualites/lire-nvidia-confirme-etre-compromis-a-la-suite-d-une-cyberattaque-85991.html

Voici les principales cybermenaces auxquelles les Français sont confrontés au quotidien

https://www.01net.com/actualites/voici-les-principales-cybermenaces-auxquelles-les-francais-sont-confrontes-au-quotidien-2055460.html

Après Nvidia, Samsung se fait dérober une quantité considérable de données sensibles

https://www.01net.com/actualites/apres-nvidia-samsung-se-fait-derober-une-quantite-considerable-de-donnees-sensibles-2055392.html*

De nouveau une faille chez Sony

Un cheval de Troie a été découvert sur le Play Store... dans une application antivirus

https://www.01net.com/actualites/un-cheval-de-troie-a-ete-decouvert-sur-le-play-store-dans-une-application-antivirus-2055374.html

Mozilla de nouveau vulnérable

Mozilla corrige deux failles zero-day dans Firefox, il est urgent de mettre à jour le navigateur

https://www.01net.com/actualites/mozilla-corrige-deux-failles-zero-day-dans-firefox-il-est-urgent-de-mettre-a-jour-le-navigateur-2055364.html

Chez Samsung deuxième faille en un court laps de temps

Samsung : des failles cryptographiques découvertes dans plus de 100 millions de smartphones

https://www.01net.com/actualites/samsung-des-failles-cryptographiques-decouvertes-dans-plus-de-100millions-de-smartphones-2054968.html

Google de nouveau pointé du doigt pour son manque de securité

Android : un dangereux cheval de Troie bancaire découvert sur Google Play

https://www.01net.com/actualites/android-un-dangereux-cheval-de-troie-bancaire-decouvert-sur-google-play-2054925.html

Faille dans la cryptomonnaie

Cryptomonnaie : une faille béante permettait de créer des tokens à l'infini

https://www.01net.com/actualites/cryptomonnaie-une-faille-beante-permettait-de-creer-des-tokens-a-l-infini-2054692.html

Apple corrige en urgence une faille zero-day dans son navigateur

https://www.01net.com/actualites/apple-corrige-en-urgence-une-faille-zero-day-dans-son-navigateur-2054574.html

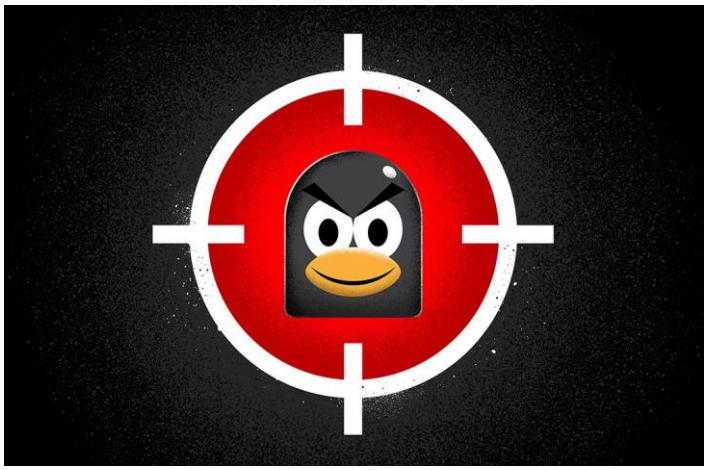
Brata, le malware bancaire qui efface toutes vos données... après les avoir volées

https://www.01net.com/actualites/brata-le-malware-bancaire-qui-efface-toutes-vos-donnees-apres-les-avoir-volees-2054187.html

Encore une fois google

Les mots de passe enregistrés sur Google Chrome ne sont pas à l'abri des cyberattaques, la plateforme pourrait être à l'origine de la récente hausse observée des cyberattaques, selon ESET

http://securite.developpez.com/actu/331806/Les-mots-de-passe-enregistres-sur-Google-Chrome-ne-sont-pas-a-l-abri-des-cyberattaques-la-plateforme-pourrait-etre-a-l-origine-de-la-recente-hausse-observee-des-cyberattaques-selon-ESET/



Linux est victime de la vulnérabilité la plus grave depuis des années, Dirty Pipe permet à un attaquant d'installer des portes dérobées, de modifier des scripts, etc.

https://linux.developpez.com/actu/331693/Linux-est-victime-de-la-vulnerabilite-la-plus-grave-depuis-des-annees-Dirty-Pipe-permet-a-un-attaquant-d-installer-des-portes-derobees-de-modifier-des-scripts-etc/