Revue d'actualité de l'OSSIR

8 mars 2022

*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

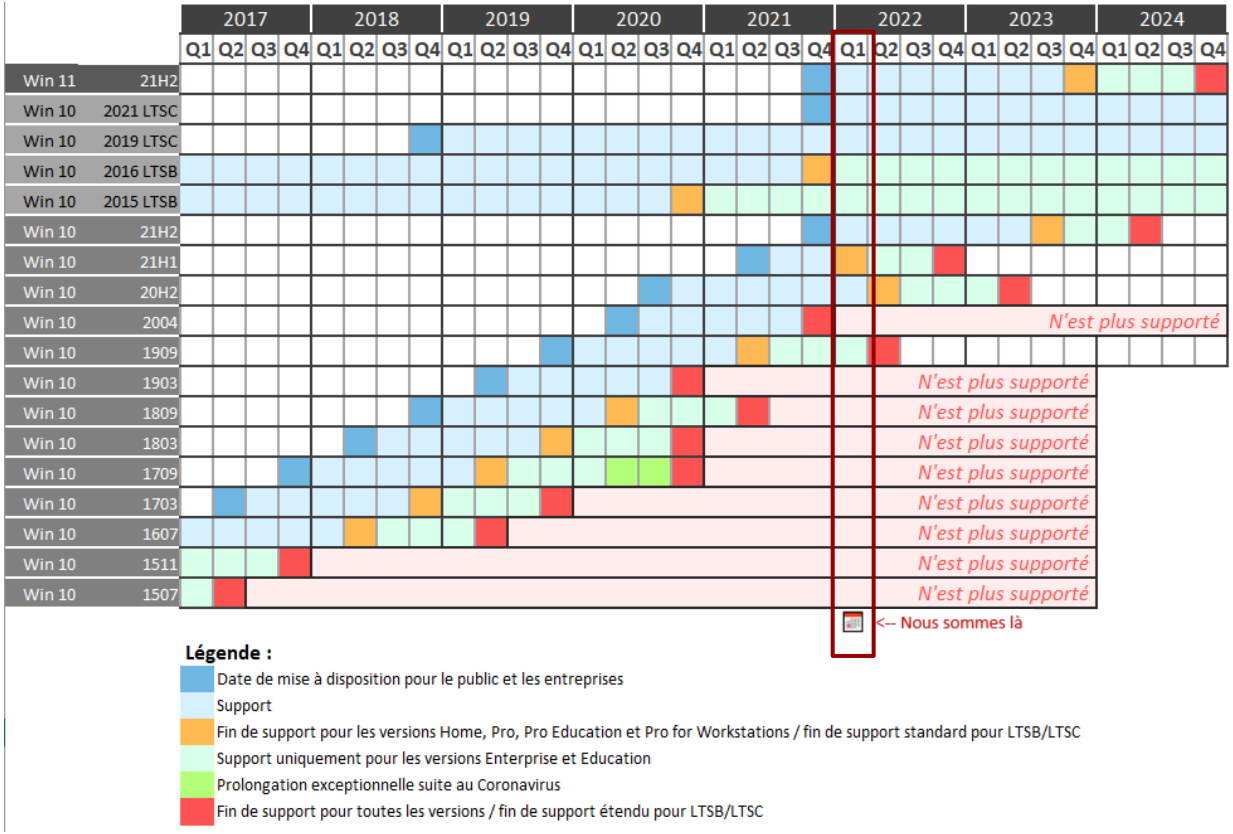
Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin Microsoft de février 2022

- 52 vulnérabilités avec en particulier :
  - Exécution de code à l'ouverture d'un fichier RTF dans **Word** (CVE-2022-21971)
    - Exploité dans la nature
    - PoC : https://github.com/0vercl0k/CVE-2022-21971
  - Exécution de code avec authentification sur **Sharepoint** par désérialisation (CVE-2022-22005)
    - PoC : https://hnd3884.github.io/posts/cve-2022-22005-microsoft-sharepoint-RCE/
  - Exécution de code à distance sur le **DNS** (CVE-2022-21984)
  - Elévation de privilèges, uniquement sur **Windows 11** (CVE-2022-21996)
  - Exécutions de code à la lecture d'une vidéo **HEVC** (CVE-2022-21844, CVE-2022-21926, CVE-2022-21927)
  - Encore des élévations de privilèges sur le **spooler d'impression** (CVE-2022-22717, CVE-2022-22718, CVE-2022-21997, CVE-2022-21999)
  - Evasion d'une machine virtuelle sur **Hyper-V** (CVE-2022-21995)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



Sortie	Home, Pro	Entreprise
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	?
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	jeudi 13 juillet 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

Failles / Bulletins / Advisories
Microsoft - Divers

eBPF bientôt sous Windows

- extended Berkeley **Packet** Filter
  - Exécution de routines noyau sans avoir à recompiler, comme une sorte de machine virtuelle
  - Très performant
  - “Packet” !!?
- Source d’exécution de code sous Linux

https://thenewstack.io/microsoft-brings-ebpf-to-windows/

Failles / Bulletins / Advisories
Systèmes

Dirty Pipe, élévation de privilèges sur linux>5.8 (CVE-2022-0847)

- Découverte par hasard du fait d'une erreur de CRC avec gzip
  - Ecriture sur un fichier ZIP par un processus qui n'en avait pas le droit
- Intervient lors du ré-assemblement de pages mémoire (splice())
- Permet d'écrire dans :
  - Un fichier en Read Only (/etc/passwd 😂) https://twitter.com/phithon_xg/status/1500902906916081666
  - Une partition montée en Read Only !!? (fichier "immuable")

https://dirtypipe.cm4all.com/

SMB, exécution de code à distance sans authentification (CVE-2021-44142)

- Avec les privilèges du processus smbd
- Présenté à Pwn2Own Austin 2021 qui avait pour cibles : NAS, Smartphones, Imprimantes…
  - Pwn2Own : https://www.zerodayinitiative.com/blog/2022/2/1/cve-2021-44142-details-on-a-samba-code-execution-bug-demonstrated-at-pwn2own-austin
  - Article : https://0xsha.io/blog/a-samba-horror-story-cve-2021-44142
  - PoC : https://gist.github.com/0xsha/0859033e1777490576923a27fbcd23ac

Failles / Bulletins / Advisories
Systèmes

Apple mac T2, récupération (ou presque) de la clef de chiffrement du disque

- Simple brute force “hors ligne”, efficace contre une clef faible…
  - Performance de 65k pass/sec. << c’est pas ouf ! >>
- Contournement de la limite de tentatives (car “hors ligne”)
  - Sinon, vous avez hashcat 👍

https://9to5mac.com/2022/02/17/t2-mac-security-vulnerability-passware/

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Firefox, 2 vulnérabilités exploitées dans la nature

- CVE-2022-26485, exécution de code à l’ouverture d’un XSLT
- CVE-2022-26486, évasion de la sandbox à partir des appels au WebGPU

https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Github cmark-gfm, exécution de code (CVE-2022-24724)

- Dépassement d'entier lors du traitement de markdown
  - Si un tableau contient plus de 2^16 colonnes (UINT16_MAX)

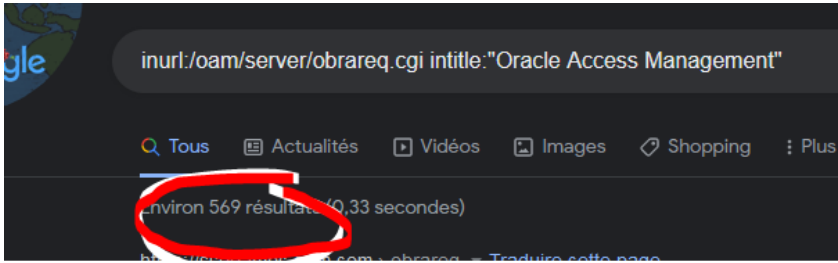
https://github.com/github/cmark-gfm/security/advisories/GHSA-mc3g-88wq-6f4x

ZAP est vulnérable à Log4J

https://www.zaproxy.org/docs/desktop/releases/2.11.1/

Oracle Access Manager (OAM), exécution de code sans authentification (CVE-2021-35587)

- Démo : https://www.youtube.com/watch?v=pkoHPJSAB2o
- Article bientôt publié…



Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco

15 bulletins, dont **2 critiques**

- Cisco Redundancy Configuration Manager
  - CVE-2022-20649, RCE (CVSS:9.0)

- Cisco Small Business RV Series Routers
  - CVE-2022-20699, RCE sur le VPN (CVSS:10.0)
  - CVE-2022-20700, RCE (CVSS:10.0)
  - CVE-2022-20703, élévation locale de privilèges (CVSS:9.0)

https://tools.cisco.com/security/center/publicationListing.x

Failles / Bulletins / Advisories
Smartphones (principales failles)

Android avec Qualcomm SnapDragon, exécution de code à distance (CVE-2021-1965)

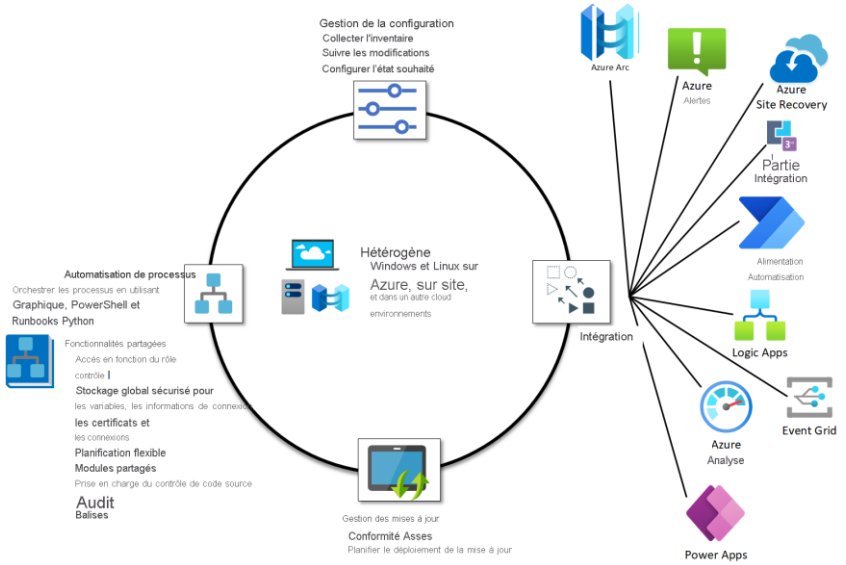
- Qualifiée de “Zéro Clic”
- Vulnérabilité dans les pilotes WiFi
  - PoC : https://github.com/parsdefense/CVE-2021-1965

Failles / Bulletins / Advisories
Autre (principales failles)

Azure Automation Account, récupération des jetons des autres clients

- Exécution (normale) de code Python à distance (~PaaS / serverless)
- Accès au service d'autorisation "des autres clients" permettant de récupérer leurs jetons
  - Corrigé par l'ajout d'un entête d'identification (X-IDENTIFY-HEADER)

https://orca.security/resources/blog/autowarp-microsoft-azure-automation-service-vulnerability/



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Ciblage du secteur Indien de l'énergie

- Par un groupe "à priori" Chinois (RedEcho)

https://www.fbcinc.com/source/virtualhall_images/NLIT_June_21/Recorded_Future/cta-2021-0228.pdf

Arrêt d'une usine de Toyota suite à la compromission d'un fournisseur

- Retard de livraison de prêt de 13k voitures

https://www.rfi.fr/en/toyota-halts-japan-plants-after-reported-cyber-attack

Piratage de firewall WatchGuard par Cyclops Blink (Sandworm)

- Opération menée par une agence étatique pour construire son botnet
  - Relais pour d'autres attaques
- Compromission des firewalls et VPN par les interfaces d'admin exposées sur Internet 😰

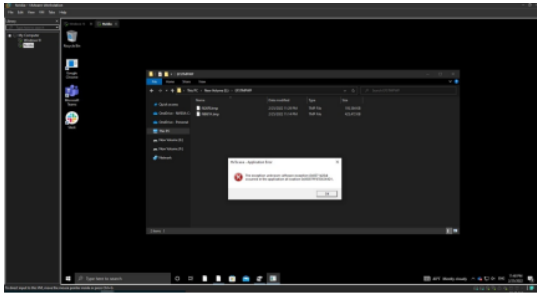
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

https://www.watchguard.com/fr/wgrd-news/blog/mesures-de-remediation-et-de-detection-du-botnet-cyclops-blink-parraine-par-des

Piratages, Malwares, spam, fraudes et DDoS
Malware

Le groupe Lapsus$ pirate Nvidia

- Vol de 1To de données dont :
  - Codes sources *(partiellement publié)*
  - Condensats NTLM des utilisateurs + certains mots de passe *(publiés)*
  - Certificat + clef privée, périmé mais valides pour des pilotes Windows
    - Mimikatz https://www.virustotal.com/gui/file/9d123f8ca1a24ba215deb9968483d40b5d7a69feee7342562407c42ed4e09cf7/details
    - Kernel Driver Utility https://www.virustotal.com/gui/file/0e1638b37df11845253ee8b2188fdb199abe06bb768220c25c30e6a8ef4f9dee/details
- Chantage demandant à Nvidia de rendre ses pilotes open source
- Lapsus$ accuse Nvidia d'un "hack back"
  - Leur VM utilisée pour se connecter en VPN a été enrôlée par le MDM
  - Et le disque a été chiffré 🥸
    - "Hack back" ou simple déploiement de la politique de chiffrement de disque suite à l'enrôlement ? 🤣🤣🤣



EVERYONE!!! NVIDIA ARE CRIMINALS!!!!!!!!!

SOME DAYS AGO WE CONDUCTED A ATTACK AGAINST NVIDIA AND STOLE 1TB OF CONFIDENTIAL DATA!!!!!!

TODAY WE WOKE UP AND WE FOUND NVIDIA SCUM HAD ATTACKED **OUR** MACHINE WITH RANSOMWARE.....

LUCKILY WE HAD A BACKUP BUT WHY THE FUCK THEY THINK THEY CAN CONNECT TO OUR PRIVATE MACHINE AND INSTALL RANSOMWARE!!!!!!!!!!

245 07:02

Piratages, Malwares, spam, fraudes et DDoS
Malware

Le groupe Lapsus$ pirate Samsung

- Vol de 200Go de données dont :
  - Codes sources Security/Defense/Knox/Bootloader/TrustedApps
  - Bootloader
  - Les dépots github

- Les groupes Telegram associés
  - ⚠ Ne pas se connecter avec son téléphone perso/pro
  - ⚠ Masquer son IP
  - ⚠ Eviter d'utiliser le client lourd
  - ⚠ Bien configurer (durcir) Telegram avant de se connecter

    https://t.me/minsaudebr

    https://t.me/saudechat

Piratages, Malwares, spam, fraudes et DDoS
Malware

Le groupe Conti piraté par… on ne sait pas

- Publication de :
  - Leur vidéos de formation
  - Leur documentation
  - Leur code source
  - Leur communications Rocket Chat, forum Trickbot
  - …

  https://share.vx-underground.org/Conti/

  https://github.com/TheParmak/conti-leaks-englished (version traduite mais incomplète)
- Déjà une fuite en 2021 avec leurs guides/manuels
- Plusieurs entreprises avaient déjà des “shell” sur leurs serveurs

  https://twitter.com/pancak3lullz/status/1461708117348163587
- Est-ce lié à leur annonce de soutien au gouvernement Russe ?

  https://twitter.com/ido_cohen2/status/1497244678932111364?s=11

Piratages, Malwares, spam, fraudes et DDoS
Malware

Le groupe Conti, son leak et son contenu

- Beaucoup de demande d'aide des opérateurs (port RDP, sortir de VIM …)
  - Les cybercriminels ont eux aussi du mal à recruter
  - Ces opérateurs à $500 suivent les procédures et cliquent
- Ils en savent très peu sur leurs victimes
  - Permet de mieux comprendre certaines négociations "lunaires"
- Les grands classiques :
  - Shodan (en payant) pour cartographier
  - Cobalt Strike (en payant) et font des classiques :
    - Kerberoasting
    - Récupération des mots de passe DPAPI
    - Utilisation d'exploit avec des outils open source
    - Path the Hash avec Mimikatz
  - EDR (en payant) pour les contourner
  - SpiderFoot pour de l'empreinte externe
  - …

https://www.lemagit.fr/actualites/252514027/Conti-dans-les-coulisses-dun-cyber-gang-aux-allures-de-PME

- Pour aller plus loin :

```
find ./conti -type f -regextype posix-extended -regex '.*([0-9]+-){3}.*\.json'|xargs printf "jq -r '.messages[].msg' %q|grep -i 'beacon>'\n"|parallel -u -j 4 {}
find ./conti -type f -name "*.json"|grep -P '\d+-\d+-\d+.*\.json'|while read i; do cat $i|jq -r '.messages[].msg'|grep 'beacon> shell';
done
```

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Un nouveau “Wiper” déployé mais sans activation massive

- “Wiper” déployé par GPO
  - Détruit la MBR
- Activé sur quelques cibles mais pas toutes
- Compromissions en sommeil depuis nov. 2021

https://twitter.com/campuscodi/status/1496592955838275589?s=11

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Blue Team Un émulateur Apple iOS basé sur QEMU

- A tester !
- `<<ça fonctionne bien mais je vais rester sur Corellium pour l'instant>>`

https://github.com/TrungNguyen1909/qemu-t8030

Blue Team AsureHunter, chasse aux attaquants dans Azure (Threat Hunting)

- Permet de vérifier des "playbook" sur les "audit log" Azure
- 5 "playbook" fournis

https://github.com/darkquasar/AzureHunter

Blue Team rappel, identifier s'il y'a eu activation de Macro

- Dans :

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\<version>\<logiciel>\Security\Trusted Documents`

- En attendant que Microsoft désactive les Macros 😎

Red Team Contourner les EDR grâce à EnumSystemGeoID( )

- API disposant d'un "callback"
  - Avec un PoC en Rust 😱

https://github.com/HuskyHacks/RustyProcessInjectors/blob/master/EnumSystemGeoID/src/main.rs

Business et Politique

Business
Monde

NeoSoft rachète CONIX

- CONIX spécialiste cybersécurité et en particulier SOC PDIS/PRIS

  https://agence-api.ouest-france.fr/article/avec-le-rachat-de-conix-neo-soft-renforce-son-expertise-en-cybersecurite

Google rachète Mandiant pour $5 Mds

- Tout le monde pariait sur Microsoft…
- Revente par FireEye du fait de problèmes de visibilité de l'offre

  https://www.securityweek.com/google-acquire-mandiant-54-billion-cash

Droit / Juridique / Politique
Monde

Microsoft gagne le procès sur le brevet de rANS

- Asymmetric Numeral System est sans brevet (volonté de l'inventeur)
- rANS est une variante de ANS
- ANS est utilisé dans JPEG XL (meilleur que JPEG), par Nvidia…

https://www.theregister.com/2022/02/17/microsoft_ans_patent/

Le cyber score est voté au sénat

- Mise en application… ???

https://www.nextinpact.com/article/49887/cyberscore-vers-vote-conforme-proposition-loi-au-senat

ANSSI, publication des recommandations pour la journalisation

- Bonnes pratiques de configuration Windows et Active Directory
- Pas la liste des "events" à surveiller

https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-journalisation-des-systemes-microsoft-windows-en-environnement-active-directory/

Droit / Juridique / Politique
Monde

Saisie du site Raidforums.com le 25 février

- Et ses miroirs rf.ws , raid.lol et rfmirror.com
  - Remplacé par une page d'hameçonnage

https://twitter.com/Janomine/status/1499453777648234501

- Egalement le cas pour nulled.to

https://twitter.com/PogoWasRight/status/1499730326364602372

- Quel avenir pour les services de veille du Darknet !!?
  - 95% se content de surveiller raid, eleaks et xss 🤣

Conférences

Conférences

Passée

- À faire…

A venir

- À faire…

Spécial Cyber-guerre

Divers / Trolls velus

La cyber guerre n’existe pas

- Démoraliser, déstabiliser, distraire, intimider… : **oui**
- Faire la guerre : **non**

https://www.lesnumeriques.com/vie-du-net/conflit-en-ukraine-peut-on-vraiment-parler-de-cyberguerre-a177805.html

Donc :

- Pas de panique
- Ne stressez pas vos équipes SOC/CERT pour rien
- Appliquez les bonnes pratiques…
  - A minima : https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/
  - Mais surtout : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Mais quand les militaires sont à vos frontières…

- Contactez les sur Tinder

https://www.slate.fr/story/223998/militaires-soldats-russe-tinder-ukraine-russie-guerre-drague

Divers / Trolls velus

L’Ukraine appelle les hackeurs à la défendre

https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/

Organisation de civils pour pirater des cibles adverses

- Civils ET cybercriminels
- Défacement, DDoS, rançonnage…

https://twitter.com/Cyberknow20/status/1499376169237417985

GROUP	SUPPORTING	ATTACKS	COMM	LOC	DATE STA
AgainstTheWest	Ukraine	Data Breach/Ranso	Twitter	France	2021
Belarusian Cyber Partisans	Ukraine/Free Belar	Ransomware	Twitter	Belarus	2020
Anonymous	Ukraine	DDoS	Twitter	Global	2022
GhostSec	Ukraine	Hack	Telegram	UNK	2022
IT Army of Ukraine	Ukraine	DDoS/Hack	Twitter	Ukraine	2022
KelvinSecurity HackingTeam	Ukraine	Hack	Telegram	UNK	2022
BlackHawks	Ukraine	DDoS	Twitter	Georgia	2022
Anon Liberland & PWN-BAR	Ukraine	DDoS	Twitter	UNK	2022
RaidForums Admin	Ukraine	Sanction	Raidforu	UNK	2022
Netsec	UNK	Hack	Twitter	UNK	2022
Free Civilian	Russia	Data Breach	Onion	UNK	2022
CoomingProject	Russia	Data Breach	Onion	France	2022
Conti Ransomware Gang	UNK	Ransomware	Onion	Global	2022
The Red Bandits	Russia	Data Breach/Hack	Twitter	Russia	2022
GhostWriter UNC1151	Russia	Hack/Disinformatio	UNK	Belarus	UNK
SandWorm	Russia	Hack/DDoS/Disinfo	UNK	Russia	UNK
Gamaredon	Russia	Hack	UNK	Russia	UNK
28-Feb					
GNG	Ukraine	DDoS	Twitter	Georgia	2022
NB65	Ukraine	Hack	Twitter	UNK	2022
ECO	UNK	UNK	Twitter	UNK	2022
RaidForums2	Ukraine	DDoS/Leaks	Twitter	UNK	2022
ContiLeaks	Ukraine	Data Breach	Twitter	UNK	2022
SHDWSec	Ukraine	Hack/Activism	Twitter	Global	2022
GhostClan	Ukraine	Hack/DDoS	Telegram	Global	2022
Eye of the Storm	Ukraine/Free Belar	Hack	Twitter	Global	2022
1-Mar					
Root User	Ukraine	Radio	Twitter	Ukraine	2022
DeepNetAnon	Ukraine	Radio	Twitter	UNK	2022
FreeUkraineNow	Ukraine	DDoS/Hack	Twitter	Ukraine	2022
1LevelCrew	Ukraine	DDoS	Twitter	UNK	2022
IT Army of Ukraine Psyops	Ukraine	Disinformation	Twitter	Ukraine	2022
Hydra UG	Ukraine	Radio/data breach	Twitter	UNK	2022
Zatoichi	Russia	Disinformation	Twitter	Russia	2022
Stormous Ransomware	Russia	Ransomware	Telegram	UNK	2022
2-Mar					
Digital Cobra Gang	Russia	Hack	Twitter	UNK	2022
N3UR0515	Ukraine	DDoS	Twitter	UNK	2022
PuckArks	Ukraine	DDoS/Hack	Twitter	UNK	2022
Secjuice	Ukraine	OSINT/PsyOps	Twitter	UK	2022
IT_G33Ks	Ukraine	DDoS/Hack	Twitter	Switzerland	2022
GrenXPaRTa_9haan	Ukraine	Hack	Twitter	US	2022
YourAnonNews	Ukraine	DDoS/Hack	Twitter	Global	2022
DDoSecrets	Ukraine	DDoS/Hack	Twitter	US	UNK
LiteMods	Ukraine	DDoS/Hack	Twitter	Global	UNK
Xaknet	Russia	Hack	Site	Russia	2022
3-Mar					
v0g3lSec	Ukraine	Hack	Twitter	UNK	2022
0xGUndala	Ukraine	DDoS/Hack	Twitter	UNK	2022
killnet	Russia	DDoS/Hack	Telegram	Russia	2022
BlueHornet (ATW)	Ukraine	Hack	Twitter	France	2022
Hidden Cobra (RUMOUR)	Russia	DDoS/Hack	UNK	Russia	2022
AgainstTheWest2	Ukraine	Hack	Twitter	France	2022

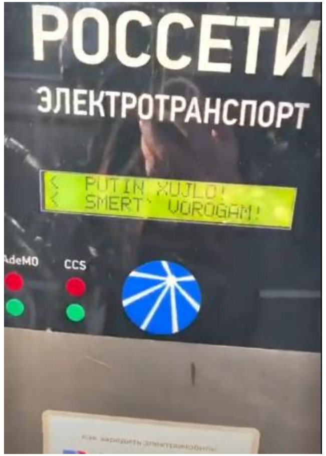
Compromission de

- Stations essences Russes

https://twitter.com/vxunderground/status/1498284587180568578

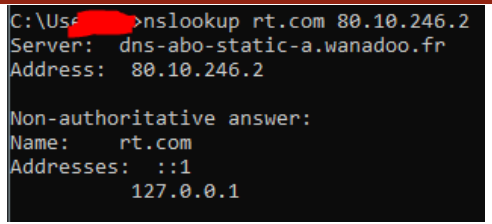
- Chaine de télé Russe

https://twitter.com/YourAnonTV/status/1497678663046905863



Divers / Trolls velus

Coupure des DNS de RT en France



- Depuis nos opérateurs nationaux
  https://framagit.org/-/snippets/6522
- RT dont les demandes de cartes de presse ont été rejetées
  https://www.lalettrea.fr/medias_audiovisuel/2022/03/08/rt-france--les-nouvelles-demandes-de-carte-de-presse-seront-refusees,109738667-bre

Kasperky victime colatérale

- Mauvaise lecture de nombreux médias du rapport de l'ANSSI
  https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

  [...] les outils de la société Kaspersky, peut être **questionnée** du fait de leur lien avec la Russie. A ce stade, **aucun élément objectif ne justifie** de faire évoluer l'évaluation du niveau de qualité [...]

La Russie va (à nouveau) tester une déconnexion partielle d'Internet

- Prévue pour le 11 mars
  https://twitter.com/sbudnitsky/status/1500635341769818117
- Peu d'impact sur les mises à jour Kasperky, ils ont prévu le coup

Divers / Trolls velus

Télégram au coeur du conflit

- Et le monde découvre que l'app ne chiffre pas par défaut les communications
  - Entre les utilisateurs, en supplément du SSL/TLS de transport

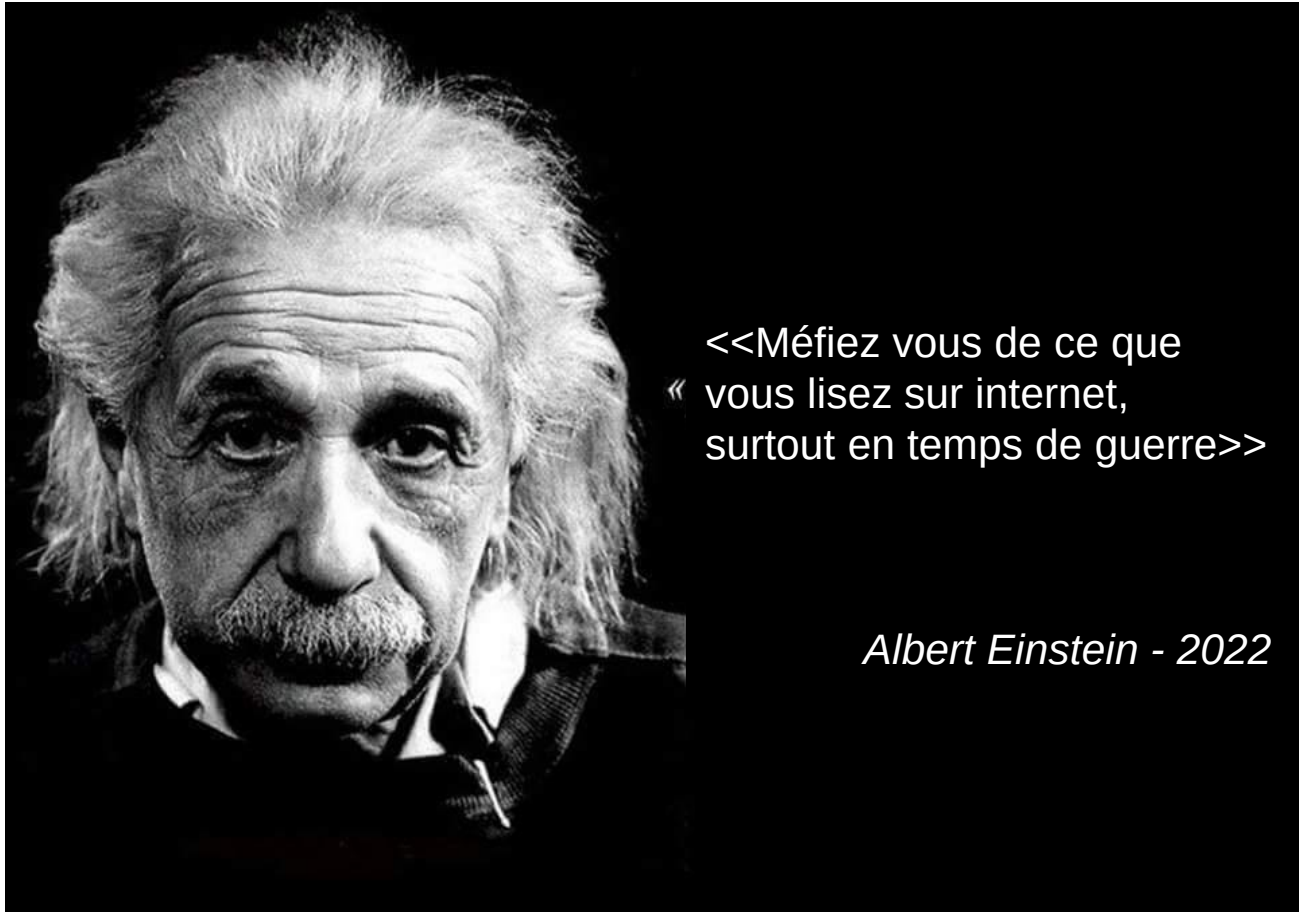
    https://www.eff.org/deeplinks/2022/03/telegram-harm-reduction-users-russia-and-ukraine
- Ou uniquement ceux ne suivant pas Quarkslab, ni l'OSSIR, ni l'EFF, ni "Secure Messaging Apps Comparison" … tout cela date de 2020

  https://twitter.com/quarkslab/status/1126859484062736384

  https://www.eff.org/node/101713/

  https://www.securemessagingapps.com/

Divers / Trolls velus



Divers / Trolls velus

Divers / Trolls velus

Quand tu confonds condensat et signature authenticode

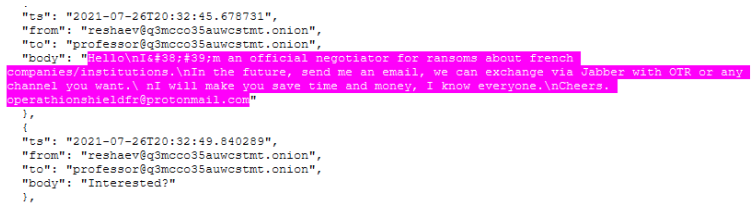
- SHA256(fichier.exe) != fichier.exe:authenticode.sha256

  https://twitter.com/0gtweet/status/1499719474609635329?s=11

Leak Conti, les échanges avec le “négociateur” français

- Avant sa garde à vue…

  https://twitter.com/campuscodi/status/1498436201300344833?s=11



Kaspersky Security Center

- Dans le doute, pensez à bien sécuriser la console de gestion KSC
- Si vous avez accès à la console et qu’elle utilise le compte local KlSvScv…
  - Il est possible de récupérer le mot de passe et orchestrer tous les antivirus

  https://twitter.com/snovvcrash/status/1494660022583840774?s=11

Divers / Trolls velus

Bloquer les IP du pays ennemi

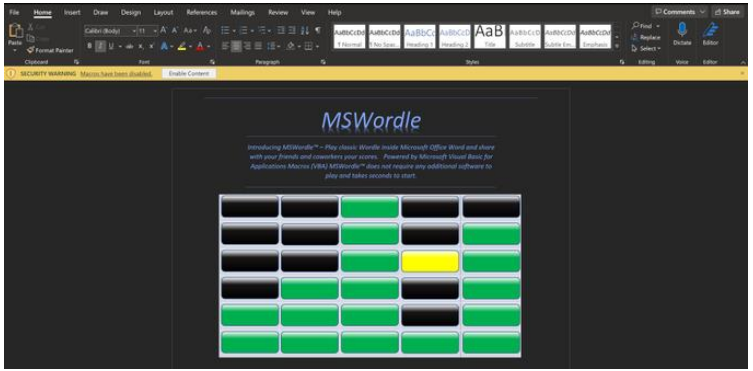
- IP brutes, .htaccess, règles pour firewall Juniper/Iptables…
  - Utilité TRES limitées car les attaquants passent par des relais 😁

https://www.countryipblocks.net/acl.php

Les cybercriminels utilisent Wordle/Sutom pour leurs hameçonnage

- Ils suivent les modes…

https://twitter.com/laughing_mantis/status/1494458289920221184?s=11



Prochaines réunions

Prochaine réunion

- 12 avril 2022… toujours en visio

After Work

- Prochainement…

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?