

Cybersécurité

Qui fait quoi ? Comment se protéger ?

Guillaume MULLER & Philippe BEAUNE

<2024-01-18 Thu>

1 Introduction

2 Ordinateur

3 Réseau

4 Conclusion

Guillaume MULLER

- 🖥️ Docteur ès Informatique
- 👤 Enseignant-Chercheur à Mines Saint-Étienne
- 🧠 Intelligence Artificielle, ⚙️ Cyber-Sécurité
- Fraîchement recruté














Philippe BEAUNE

- 🖥️ Ingénieur et Docteur ès Informatique
- 👤 ex-Enseignant-Chercheur à Mines Saint-Étienne
- 🧠 Intelligence Artificielle
- Fraîchement à la retraite 😊
















- Quels sont vos domaines d'intérêt ?














- Quels sont vos domaines d'intérêt ?
- Êtes-vous utilisateurs-trices d'outils numériques ?
 -  Ordinateur /  SmartPhone /  Tablette ?

- Quels sont vos domaines d'intérêt ?
- Êtes-vous utilisateurs-trices d'outils numériques ?
 -  Ordinateur /  SmartPhone /  Tablette ?
 -  Windows -  Mac -  Linux /  iOS -  Android ?














Qui êtes vous?

- Quels sont vos domaines d'intérêt ?
- Êtes-vous utilisateurs-trices d'outils numériques ?
 -  Ordinateur /  SmartPhone /  Tablette ?
 -  Windows -  Mac -  Linux /  iOS -  Android ?
- Êtes-vous utilisateurs-trices de réseaux sociaux      ?

Qui êtes vous?

- Quels sont vos domaines d'intérêt ?
- Êtes-vous utilisateurs-trices d'outils numériques ?
 -  Ordinateur /  SmartPhone /  Tablette ?
 -  Windows -  Mac -  Linux /  iOS -  Android ?
- Êtes-vous utilisateurs-trices de réseaux sociaux      ?
- Que savez-vous de la Cyber-Sécurité ?
 - Dernières Attaques/Failles/Problèmes ?

Qui êtes vous?

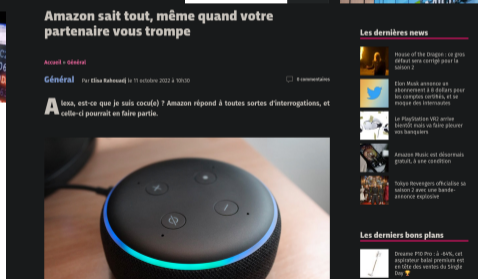
- Quels sont vos domaines d'intérêt ?
- Êtes-vous utilisateurs-trices d'outils numériques ?
 -  Ordinateur /  SmartPhone /  Tablette ?
 -  Windows -  Mac -  Linux /  iOS -  Android ?
- Êtes-vous utilisateurs-trices de réseaux sociaux      ?
- Que savez-vous de la Cyber-Sécurité ?
 - Dernières Attaques/Failles/Problèmes ?
- Qu'attendez-vous de cette conférence ?



source

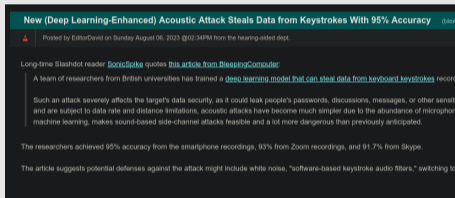


source



source

"reNouveau de l'ancien"




source

"Erreurs" de conception


Kia Challenge : le phénomène TikTok qui fait exploser les vols de voiture aux USA

Publié le 30 août 2023 à 17:10 par [Mathieu M.](#)

C'est un challenge qui prend trop d'ampleur au goût des autorités américaines : le Kia Challenge de TikTok fait de plus en plus de victimes outre-Atlantique.



Lire sur mobile



Bons Plans High-Tech

LES BONS PLANS

Apple iPad : la gamme de tablettes en promotion, mais pas que !

source

Exemples récents – 2023 – Microsoft

Microsoft Comes Under Blistering Criticism For 'Grossly Irresponsible' Security (arstechnica.com)

Posted by BeauHD on Thursday August 03, 2023 @08:02PM from the serious-cybersecurity-defects dept.

An anonymous reader quotes a report from Ars Technica:

Microsoft has once again come under blistering criticism for the security practices of Azure and its other cloud offerings, with the CE comments from Amit Yoran, chairman and CEO of Tenable, come six days after Sen. Ron Wyden (D-Ore.) blasted Microsoft for what hundreds of thousands of emails from cloud customers, including officials in the US Departments of State and Commerce. Microsoft powerful encryption key granting access to a variety of its other cloud services.

On Wednesday, Yoran took to LinkedIn to [castigate Microsoft](#) for failing to fix w managing user authentication inside large organizations. Monday's disclosure was incomplete. Microsoft set the date for providing a complete fix to September

"To give you an idea of how bad this is, our team very quickly discovered authentication. Did Microsoft quickly fix the issue that could effectively lead to the breach of tr

source

Malicious Microsoft Drivers Could Number in the Thousands, Says Cisco Talos

Posted by EditorDavid on Saturday July 15, 2023 @11:44PM from the forged-signature-limestamp dept.

An anonymous reader [shared Thursday's report from eSecurity Planet](#):

After Microsoft [warned](#) earlier this week that some drivers certified by the Windows Hardware Developer thousands.

How the security problem evolved in [a blog post](#). "Starting in Windows 10, kernel-mode drivers would no longer need to be signed by its Developer Portal. This was a change that allowed developers to sign their drivers with their own certificates. Unfortunately, one for drivers signed with certificates that expired or were invalid. This means that thousands of drivers have been developed to exploit this loophole," Neal wrote. And

Bypassing BitLocker using a cheap logic analyzer on a Lenovo laptop

Thom Holwerda 2023-08-24 Privacy Security 6 Comments

The BitLocker partition is encrypted using the Full Volume Encryption Key (FVEK). The FVEK itself is encrypted using the Volume Master Key (VMK) and stored on the disk, next to the encrypted data. This permits key rotations without re-encrypting the whole disk.

The VMK is stored in the TPM. Thus the disk can only be decrypted when booted from this computer (there is a recovery mechanism in Active Directory though).

In order to decrypt the disk, the CPU will ask that the TPM sends the VMK over the SPI bus.

The vulnerability should be obvious: at some point in the boot process, the VMK transits unencrypted between the TPM and the CPU. This means that it can be captured and used to decrypt the disk.

This seems like such an obvious design flaw, and yet, that's exactly how it works - and yes, as this article notes, you can indeed capture the VMK in-transit and decrypt the disk.

source

source

Paysage évolue sans arrêt

- Jeu du chat ("Police") et de la souris ("Attaquants")
- 2023 📈 **Augmentation des attaques**

Avant (→ ~ 2020)

Attaques assez simples

Outils très compliqués

Attaquants "Hacker" solo

Victimes

- Militaires 🎮
- Entreprises 💰



Tendances 2022-2023

Attaques compliquées (♻️, 👤+💻)

Outils simples & 🚚

Attaquants APT ^a (👥 / 🚩 / 💰)

Victimes

- ONG, 🏢, 🏠
- Opposants, **particuliers**

^aAdvanced Persistent Threat

① Introduction

② Ordinateur

③ Réseau

④ Conclusion

Ordinateur

- Attaque "Physique"
- Mots de passe
- Périphériques extérieurs (Clef USB)

Réseau

- Courriel / Web
- Téléphonie / SMS
- Objets connectés / Réseaux Sociaux

1 Introduction

2 **Ordinateur**

3 Réseau

4 Conclusion

Démontage

- Éteindre la machine @Victime
- Sortir le disque de la machine @Victime
- Connecter sur machine @Pirate ([adaptateur](#))
- Lire les fichiers comme sur une clef USB



Démo: Accès par Démontage disque ou LiveCD

Démontage

- Éteindre la machine @Victime
- Sortir le disque de la machine @Victime
- Connecter sur machine @Pirate ([adaptateur](#))
- Lire les fichiers comme sur une clef USB



LiveCD

- [Préparer une clef USB Linux démarrable](#)
- Redémarrer l'ordinateur @Victime sur la clef
- "Monter" le disque et lire les fichiers



Démontage

- Éteindre la machine @Victime
- Sortir le disque de la machine @Victime
- Connecter sur machine @Pirate ([adaptateur](#))
- Lire les fichiers comme sur une clef USB





LiveCD

- [Préparer une clef USB Linux démarrable](#)
- Redémarrer l'ordinateur @Victime sur la clef
- "Monter" le disque et lire les fichiers



SOLUTIONS

-  Surveiller l'ordinateur et  [Chiffrer le disque](#)

Démo: Cassage (Cracking) de mots de passes

Cassage

- Récupérer les fichiers SYSTEM & SAM (@Victime)

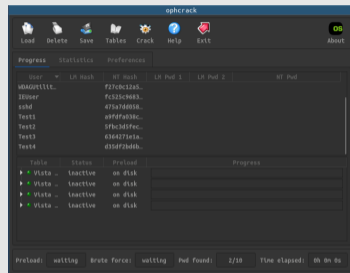
```
reg save hklm\sam c:\SAM  
reg save hklm\system c:\SYSTEM
```

- Extraire les mots de passe "chiffrés" (hash, @Pirate)

```
impacket-secretsdump -sam SAM -system SYSTEM LOCAL
```

- Casser le "chiffrement" (@Pirate)

```
ophcrack -d <tables> -e -f dump.text
```



SOLUTION

- "Verrouiller" son écran
- Mots de passe **LONG** (>10 symboles) [XKCD](#)
- Mots de passe **UNIQUES** [HavelBeenPwnd](#) & autres
- ⇒ [Gestionnaires de mots de passe \(Keepass-XC \[2\]\)](#)

Problème

- J'ai trouvé une clef USB (rue, parking, salle. . .)
- Je veux retrouver son propriétaire
- Que fais-je ?

Infection

- [RuberDucky \(vidéo\)](#)



Infection

- [RuberDucky \(vidéo\)](#)



Destruction

- [USBKiller \(vidéo\)](#)



Infection

- [RuberDucky \(vidéo\)](#)



Destruction

- [USBKiller \(vidéo\)](#)



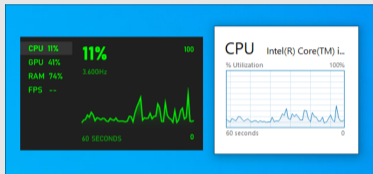
SOLUTIONS

- 👁️ Vigilance
- 🔄 Désactivation port USB (BIOS, Matérielle)

Vigilance: Suivre ce qui se passe sur son ordinateur

Surveiller

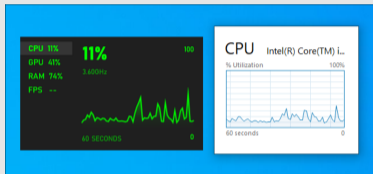
- CPU / RAM / Disque / Réseau



Vigilance: Suivre ce qui se passe sur son ordinateur

Surveiller

- CPU / RAM / Disque / Réseau



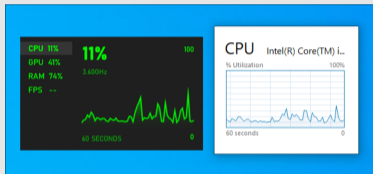
Anti-virus

- ClamAV, BitDefender, Norton, Avast, Kaspersky...
- Comparatif

Vigilance: Suivre ce qui se passe sur son ordinateur

Surveiller

- CPU / RAM / Disque / Réseau



Anti-virus

- ClamAV, BitDefender, Norton, Avast, [Kaspersky](#)...
- [Comparatif](#)

Maintenir à jour son ordinateur

- Correctifs de sécurité ("Windows Update")

1 Introduction

2 Ordinateur

3 Réseau

4 Conclusion

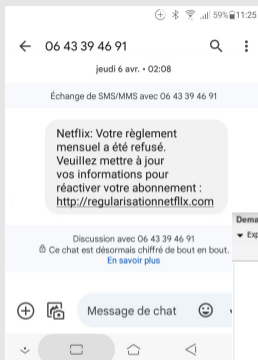
① Introduction

② Ordinateur

③ Réseau

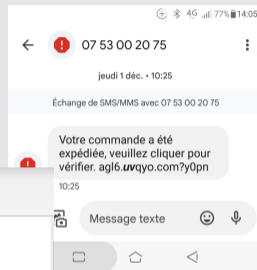
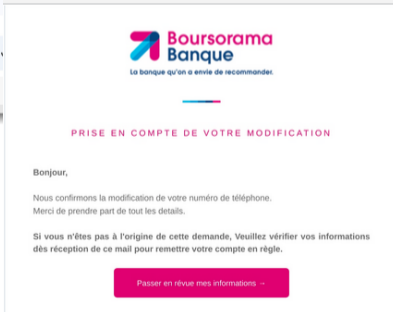
④ Conclusion

Spam/Hameçonnage par Courriel & SMS



Demande prise en compte

Expéditeur : "Boursorama" <no-reply@idoo.fr>
À: no-reply@rosso.online



Testons votre abileté à détecter les Spams/Hameçonnage

- [Test](#)

Testons votre abileté à détecter les Spams/Hameçonnage

- [Test](#)
-  ChatGPT 
 - "Arnaque au Président" [\[1\]](#) [\[2\]](#) [\[3\]](#)



Testons votre abileté à détecter les Spams/Hameçonnage

- [Test](#)
- **⚠** ChatGPT **⚠**
 - "Arnaque au Président" [\[1\]](#) [\[2\]](#) [\[3\]](#)



Points de vigilance – Résumé

- Entêtes (expéditeur **inconnu**, adresse bizarre...)
- Installation de logiciels (.exe, .bat, .vbs)
- Pièces jointes (.pdf, .docx, .xlsx, .pptx)
- Liens (incorrects, bizarres...)
- Urgence / Aguichage / Demande d'informations confidentielles
- Généricité, Fautes de français

utiliser 2nd canal

Testons votre abileté à détecter les Spams/Hameçonnage

- [Test](#)
-  ChatGPT 
 - "Arnaque au Président" [\[1\]](#) [\[2\]](#) [\[3\]](#)



SOLUTIONS

- Conseils [Gouv.fr](#)
- [HoaxKiller](#) : Tester un courriel/SMS
- [Signal Spam](#) : Signaler un courriel/SMS
- [Alias](#) : Trouver la source/stopper l'hémorragie

① Introduction

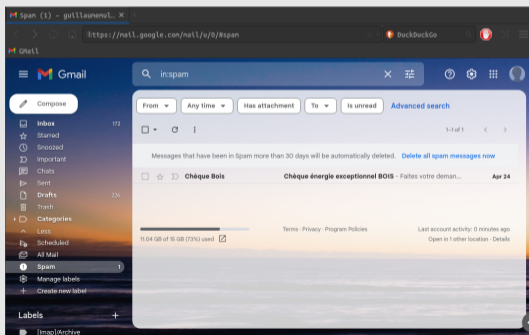
② Ordinateur

③ Réseau

④ Conclusion

Contexte

- Écran non verrouillé
- Navigateur ouvert
- Utilisateur connecté
- Remplissage Automatique activé

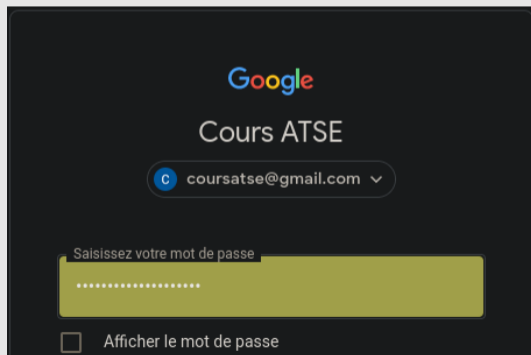


Contexte

- Écran non verrouillé
- Navigateur ouvert
- Utilisateur connecté
- Remplissage Automatique activé

Attaque

- Déconnecter la personne
- "Afficher le mot de passe"
- (ou Éditer le code : "password" → "text")
- Copier le mot de passe 📷 & log user again

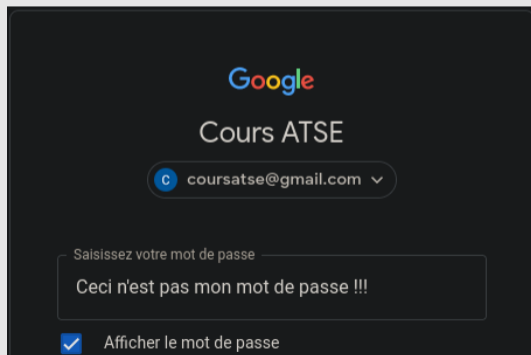


Contexte

- Écran non verrouillé
- Navigateur ouvert
- Utilisateur connecté
- Remplissage Automatique activé

Attaque

- Déconnecter la personne
- "Afficher le mot de passe"
- (ou Éditer le code : "password" → "text")
- Copier le mot de passe 📷 & log user again



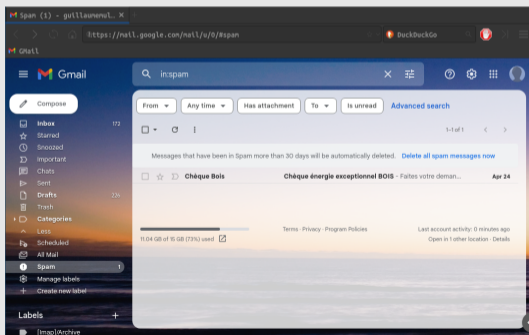
Démo: Récupération mots de passe Web

Contexte

- Écran non verrouillé
- Navigateur ouvert
- Utilisateur connecté
- Remplissage Automatique activé

Attaque

- Déconnecter la personne
- "Afficher le mot de passe"
- (ou Éditer le code : "password" → "text")
- Copier le mot de passe 📷 & log user again



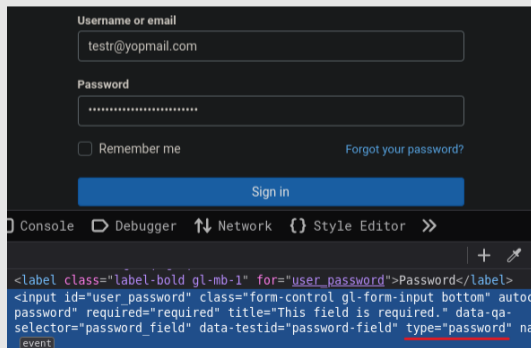
Démo: Récupération mots de passe Web

Contexte

- Écran non verrouillé
- Navigateur ouvert
- Utilisateur connecté
- Remplissage Automatique activé

Attaque

- Déconnecter la personne
- "Afficher le mot de passe"
- (ou Éditer le code : "password" → "text")
- Copier le mot de passe 📷 & log user again



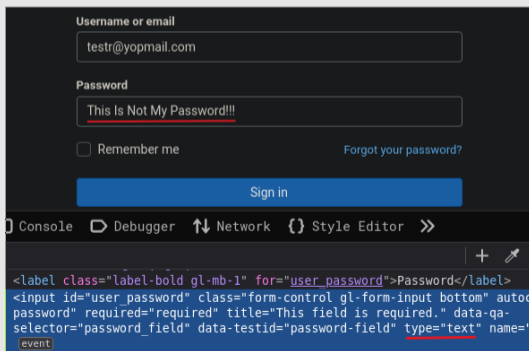
Démo: Récupération mots de passe Web

Contexte

- Écran non verrouillé
- Navigateur ouvert
- Utilisateur connecté
- Remplissage Automatique activé

Attaque

- Déconnecter la personne
- "Afficher le mot de passe"
- (ou Éditer le code : "password" → "text")
- Copier le mot de passe 📷 & log user again



SOLUTIONS

- Verrouiller son écran
- Ne pas enregistrer les mots de passe
- Ne pas configurer le remplissage automatique
- Utiliser un gestionnaire de mots de passe

① Introduction

② Ordinateur

③ Réseau

④ Conclusion

Le problème



Le problème



Principes

- *"C'est bénin" – "rien à me reprocher"*
- Qui décide ? (nouchette777)
- Quand ? (USA & Avortement)
- Numérique ↔ Jamais effacé

Le problème



Principes

- *"C'est bénin" – "rien à me reprocher"*
- Qui décide ? (nouchette777)
- Quand ? ([USA & Avortement](#))
- Numérique ↔ Jamais effacé

SOLUTIONS

- ⚠ ce qu'on met sur les réseaux sociaux (**public!!!**)
- ⚠ aux informations qu'on donne aux inconnus
- ⚠ [TikTok](#) 🎵

1 Introduction

2 Ordinateur

3 Réseau

4 Conclusion

- *C'est un équilibre à trouver : facilité d'utilisation vs. niveau de risque*

- ① Choisir avec soin ses **mots de passe** et s'assurer de leur **confidentialité**
- ② Veiller à séparer les usages professionnels des usages personnels
- ③ **Adapter les moyens** selon les données à protéger
- ④ Penser à sécuriser les **supports amovibles** et mobiles
- ⑤ Utiliser la **messagerie** avec vigilance
- ⑥ Utiliser le compte administrateur que lorsque c'est nécessaire
- ⑦ Être vigilant toujours et avoir les bons réflexes lorsqu'on veut **payer en ligne**
- ⑧ Redoubler de prudence lorsqu'on est en déplacement
- ⑨ Penser à faire des **sauvegardes régulières**
- ⑩ **Mettre à jour** vos logiciels & **antivirus**
- ⑪ Ne **télécharger que depuis les sites officiels** & sites des éditeurs
- ⑫ Protéger votre accès **Wifi** avec un **mot de passe** suffisamment complexe

① Introduction

② Ordinateur

③ Réseau

④ Conclusion



 Questions ?

 Remarques ?