

2026

Éric BERTHOMIER

unlog

10 mars 2026



Version 1.0b - Version Stagiaire

BEFORE

Zero Day : Définition

Une faille zero day (ou vulnérabilité "zero-day") est une faille de sécurité informatique **inconnue** de l'éditeur du logiciel ou du système au moment où elle est découverte ou exploitée.



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**

- Juin 2025 Découverte & exploit initial



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**

- Juin 2025 Découverte & exploit initial
 - La **Google Threat Analysis Group** identifie une faille grave dans Chrome (CVE-2025-6558).



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**

- Juin 2025 Découverte & exploit initial
 - La **Google Threat Analysis Group** identifie une faille grave dans Chrome (CVE-2025-6558).
 - Des attaquants exploitent déjà cette vulnérabilité via des pages web malveillantes.



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**

- Juin 2025 Découverte & exploit initial
 - La **Google Threat Analysis Group** identifie une faille grave dans Chrome (CVE-2025-6558).
 - Des attaquants exploitent déjà cette vulnérabilité via des pages web malveillantes.
- Juillet Août 2025 Déploiement des correctifs



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**

- Juin 2025 Découverte & exploit initial
 - La **Google Threat Analysis Group** identifie une faille grave dans Chrome (CVE-2025-6558).
 - Des attaquants exploitent déjà cette vulnérabilité via des pages web malveillantes.
- Juillet Août 2025 Déploiement des correctifs
 - Google publie une mise à jour de sécurité corrigeant la CVE-2025-6558 : Chrome doit alors être mis à jour **vers 138.0.7204.157 ou supérieur.**



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**

- Juin 2025 Découverte & exploit initial
 - La **Google Threat Analysis Group** identifie une faille grave dans Chrome (CVE-2025-6558).
 - Des attaquants exploitent déjà cette vulnérabilité via des pages web malveillantes.
- Juillet Août 2025 Déploiement des correctifs
 - Google publie une mise à jour de sécurité corrigeant la CVE-2025-6558 : Chrome doit alors être mis à jour **vers 138.0.7204.157 ou supérieur.**
 - Microsoft Edge et d'autres navigateurs basés sur Chromium reçoivent aussi les correctifs correspondants.



Exemple - CVE-2025-6558

Une vulnérabilité zero-day dans **Google Chrome** (et les navigateurs basés sur Chromium) a été **activement exploitée par des attaquants avant que tous les utilisateurs ne puissent être mis à jour.**

- Juin 2025 Découverte & exploit initial
 - La **Google Threat Analysis Group** identifie une faille grave dans Chrome (CVE-2025-6558).
 - Des attaquants exploitent déjà cette vulnérabilité via des pages web malveillantes.
- Juillet Août 2025 Déploiement des correctifs
 - Google publie une mise à jour de sécurité corrigeant la CVE-2025-6558 : Chrome doit alors être mis à jour **vers 138.0.7204.157 ou supérieur.**
 - Microsoft Edge et d'autres navigateurs basés sur Chromium reçoivent aussi les correctifs correspondants.
 - La **CISA inclut cette vulnérabilité dans sa liste KEV**, exigeant un déploiement rapide dans les infrastructures fédérales.



CVE vs CVSS vs KEV

Terme	Définition	Ce que ça ne dit PAS
CVE	Identifiant unique d'une vulnérabilité (ex : CVE-2025-1234)	Grave ou exploitée
CVSS	Score de gravité (0 à 10)	Réellement exploitée
KEV (CISA)	Liste officielle des vulnérabilités activement exploitées	Gravité technique



CVE vs CVSS vs KEV

Terme	Définition	Ce que ça ne dit PAS
CVE	Identifiant unique d'une vulnérabilité (ex : CVE-2025-1234)	Grave ou exploitée
CVSS	Score de gravité (0 à 10)	Réellement exploitée
KEV (CISA)	Liste officielle des vulnérabilités activement exploitées	Gravité technique

- CVE = Identité

<https://www.cve.org/CVERecord?id=CVE-2026-26345>

- CVSS = Gravité théorique

<https://nvd.nist.gov/vuln/detail/cve-2026-27474>

- KEV = Exploitation réelle

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



CVE vs CVSS vs KEV

Terme	Définition	Ce que ça ne dit PAS
CVE	Identifiant unique d'une vulnérabilité (ex : CVE-2025-1234)	Grave ou exploitée
CVSS	Score de gravité (0 à 10)	Réellement exploitée
KEV (CISA)	Liste officielle des vulnérabilités activement exploitées	Gravité technique

- CVE = Identité

<https://www.cve.org/CVERecord?id=CVE-2026-26345>

- CVSS = Gravité théorique

<https://nvd.nist.gov/vuln/detail/cve-2026-27474>

- KEV = Exploitation réelle

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

La gravité théorique est inutile sans contexte d'exploitation.



NOW

The Human Is The New Zero Day

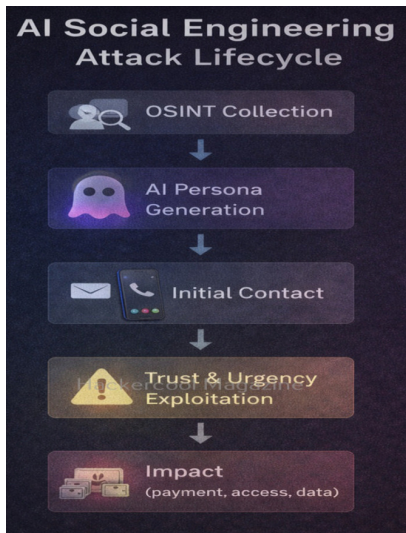
L'humain est la nouvelle faille de sécurité "Zero Day"



Identity







AI - Assistance au crime numérique



AI - Le nouveau phishing

Traditional Phishing vs AI-Generated Attacks

 Traditional Phishing	VS	 AI-Generated Attacks
 Poor grammar, limited vocabulary	→	 Flawless grammar, advanced language
 Generic, easily spotted	→	 Highly personalized and targeted
 Simple, static messages	→	 Lifelike, interactive conversations
 Easier to identify	→	 Much harder to detect

Hackercool Magazine



Where Identity Problems Appear Everywhere



Active Directory



Cloud IAM



SSO portals



VPN access



DevOps pipelines



Identity vs. Access

Identity = Who You Are



User



Service account



Admin



Role

Access = What You Can Do



Read



Write



Modify



Admin actions



Et dans les faits ...

- Les attaques ne ciblent plus seulement les logiciels, mais surtout **les utilisateurs**.



Et dans les faits ...

- Les attaques ne ciblent plus seulement les logiciels, mais surtout **les utilisateurs**.
- Les humains sont exploités comme vecteurs d'attaque, tout comme une faille 0-day :



Et dans les faits ...

- Les attaques ne ciblent plus seulement les logiciels, mais surtout **les utilisateurs**.
- Les humains sont exploités comme vecteurs d'attaque, tout comme une faille 0-day :
 - **Vol d'identité** : phishing, spear-phishing, usurpation de comptes.



Et dans les faits ...

- Les attaques ne ciblent plus seulement les logiciels, mais surtout **les utilisateurs**.
- Les humains sont exploités comme vecteurs d'attaque, tout comme une faille 0-day :
 - **Vol d'identité** : phishing, spear-phishing, usurpation de comptes.
 - **Infostealer / Malware** : logiciels malveillants qui récupèrent les données de l'utilisateur.



Et dans les faits ...

- Les attaques ne ciblent plus seulement les logiciels, mais surtout **les utilisateurs**.
- Les humains sont exploités comme vecteurs d'attaque, tout comme une faille 0-day :
 - **Vol d'identité** : phishing, spear-phishing, usurpation de comptes.
 - **Infostealer / Malware** : logiciels malveillants qui récupèrent les données de l'utilisateur.
 - **OSINT (Open Source Intelligence)** : collecte d'informations personnelles publiques pour préparer des attaques ciblées.



Et dans les faits ...

- Les attaques ne ciblent plus seulement les logiciels, mais surtout **les utilisateurs**.
- Les humains sont exploités comme vecteurs d'attaque, tout comme une faille 0-day :
 - **Vol d'identité** : phishing, spear-phishing, usurpation de comptes.
 - **Infostealer / Malware** : logiciels malveillants qui récupèrent les données de l'utilisateur.
 - **OSINT (Open Source Intelligence)** : collecte d'informations personnelles publiques pour préparer des attaques ciblées.
- Les conséquences incluent la compromission de comptes, la fuite de données sensibles et des pertes financières.



Et dans les faits ...

- Les attaques ne ciblent plus seulement les logiciels, mais surtout **les utilisateurs**.
- Les humains sont exploités comme vecteurs d'attaque, tout comme une faille 0-day :
 - **Vol d'identité** : phishing, spear-phishing, usurpation de comptes.
 - **Infostealer / Malware** : logiciels malveillants qui récupèrent les données de l'utilisateur.
 - **OSINT (Open Source Intelligence)** : collecte d'informations personnelles publiques pour préparer des attaques ciblées.
- Les conséquences incluent la compromission de comptes, la fuite de données sensibles et des pertes financières.
- L'humain est la faille la plus difficile à corriger : la sensibilisation par la compréhension et la formation restent les meilleures protections.



Biais d'attaque : cognitifs / psychologiques

- Urgence / Pression temporelle : pousse à agir sans réfléchir.



Biais d'attaque : cognitifs / psychologiques

- Urgence / Pression temporelle : pousse à agir sans réfléchir.
- Autorité : confiance dans des figures d'autorité.



Biais d'attaque : cognitifs / psychologiques

- **Urgence / Pression temporelle** : pousse à agir sans réfléchir.
- **Autorité** : confiance dans des figures d'autorité.
- **Curiosité** : clic sur contenu intrigant ou surprenant.



Biais d'attaque : cognitifs / psychologiques

- Urgence / Pression temporelle : pousse à agir sans réfléchir.
- Autorité : confiance dans des figures d'autorité.
- Curiosité : clic sur contenu intrigant ou surprenant.
- Réciprocité / Gentillesse : aider quelqu'un par réflexe.



Biais d'attaque : cognitifs / psychologiques

- Urgence / Pression temporelle : pousse à agir sans réfléchir.
- Autorité : confiance dans des figures d'autorité.
- Curiosité : clic sur contenu intrigant ou surprenant.
- Réciprocité / Gentillesse : aider quelqu'un par réflexe.
- Conformité / Pression sociale : suivre ce que font les autres.



Biais d'attaque liés à l'information (OSINT)

- **Surinformation personnelle** : collecte sur réseaux sociaux, forums.



Biais d'attaque liés à l'information (OSINT)

- **Surinformation personnelle** : collecte sur réseaux sociaux, forums.
- **Profilage comportemental** : routines, habitudes, déplacements.



Biais d'attaque liés à l'information (OSINT)

- **Surinformation personnelle** : collecte sur réseaux sociaux, forums.
- **Profilage comportemental** : routines, habitudes, déplacements.
- **Exposition involontaire** : documents ou données accessibles publiquement.



Biais d'attaque liés aux logiciels

- **Infostealer / Malware** : vol de données via logiciels malveillants.
- **Credential phishing** : imitation de pages de login.



Biais d'attaque liés aux logiciels

- **Infostealer / Malware** : vol de données via logiciels malveillants.
- **Credential phishing** : imitation de pages de login.
- **Human Beings** : faux captcha.



Biais d'attaque liés aux logiciels

- **Infostealer / Malware** : vol de données via logiciels malveillants.
- **Credential phishing** : imitation de pages de login.
- **Human Beings** : faux captcha.
- **Exploits de sécurité humaine** : mise à jour urgente trompeuse.



- **Infostealer / Malware** : vol de données via logiciels malveillants.



Défense ultime

- **Infostealer / Malware** : vol de données via logiciels malveillants.
- **Credential phishing** : imitation de pages de login.



- **Infostealer / Malware** : vol de données via logiciels malveillants.
- **Credential phishing** : imitation de pages de login.
- **Exploits de sécurité humaine** : mise à jour urgente trompeuse.



Conclusion

La vigilance mécanique est devenue insuffisante :
la **compréhension** est rendue essentielle.



Conclusion

La vigilance mécanique est devenue insuffisante :
la **compréhension** est rendue essentielle.

La défense ultime n'est plus d'appliquer des
règles,
mais de **comprendre**, analyser et anticiper.



Mise en application (1/3)

www.cuisine [redacted].com

Vérifiez que vous êtes humain en complétant l'action ci-dessous.

Vérifiez que vous êtes un humain


CLOUDFLARE
[Privacy](#) • [Terms](#)

www.cuisine [redacted].com doit vérifier la sécurité de votre connexion avant de continuer.



Mise en application (2/3)



Votre PC a rencontré un problème. Suivez les instructions de récupération ci-dessous afin de protéger vos données.

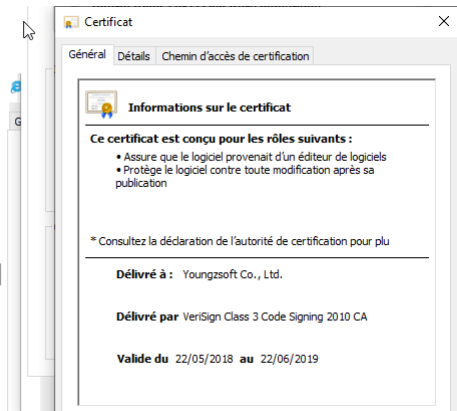
1. Maintenez la **touche Windows**  enfoncée, puis appuyez sur **R**.
2. Maintenez la touche **Ctrl** enfoncée, puis appuyez sur **V**.
3. Cliquez sur **OK** ou appuyez sur la touche **Entrée**.

Ne redémarrez pas et n'éteignez pas l'ordinateur avant d'avoir terminé ces étapes. Cela pourrait interrompre la résolution du problème.

Fix error code: 0x0000001A



Mise en application (3/3)



Vols de certificats numériques / mimétisme.
<https://www.youngzsoft.net/>



Hack'Scape Games

Pour commencer à comprendre ...



Newbie



<https://hsgnobody.ericberthomier.fr/>



Advanced



<https://hackscapegame.ericberthomier.fr/>