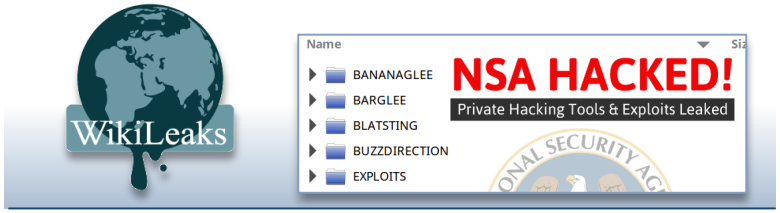
Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI

Patrice Bigeard – Délégué Ile de France
patrice.bigeard@ssi.gouv.fr

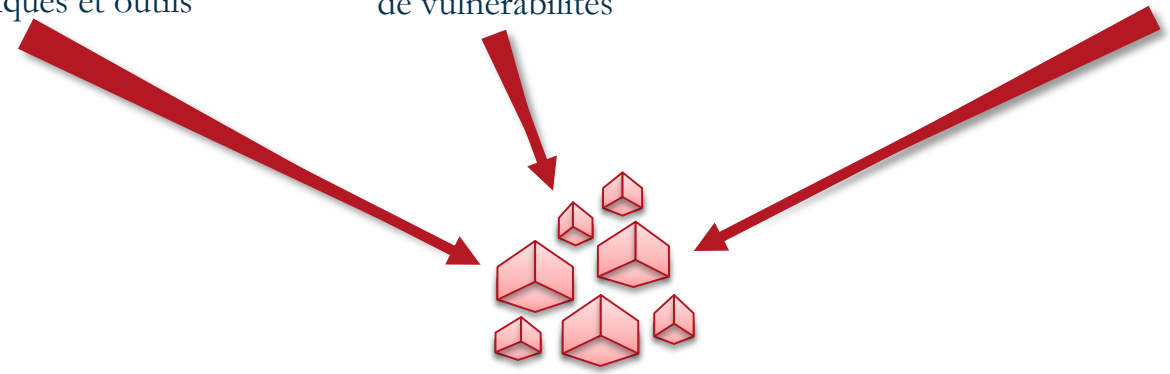
Prolifération de codes d'attaque

Publications de rapports sur techniques et outils

Découvertes et publications de vulnérabilités



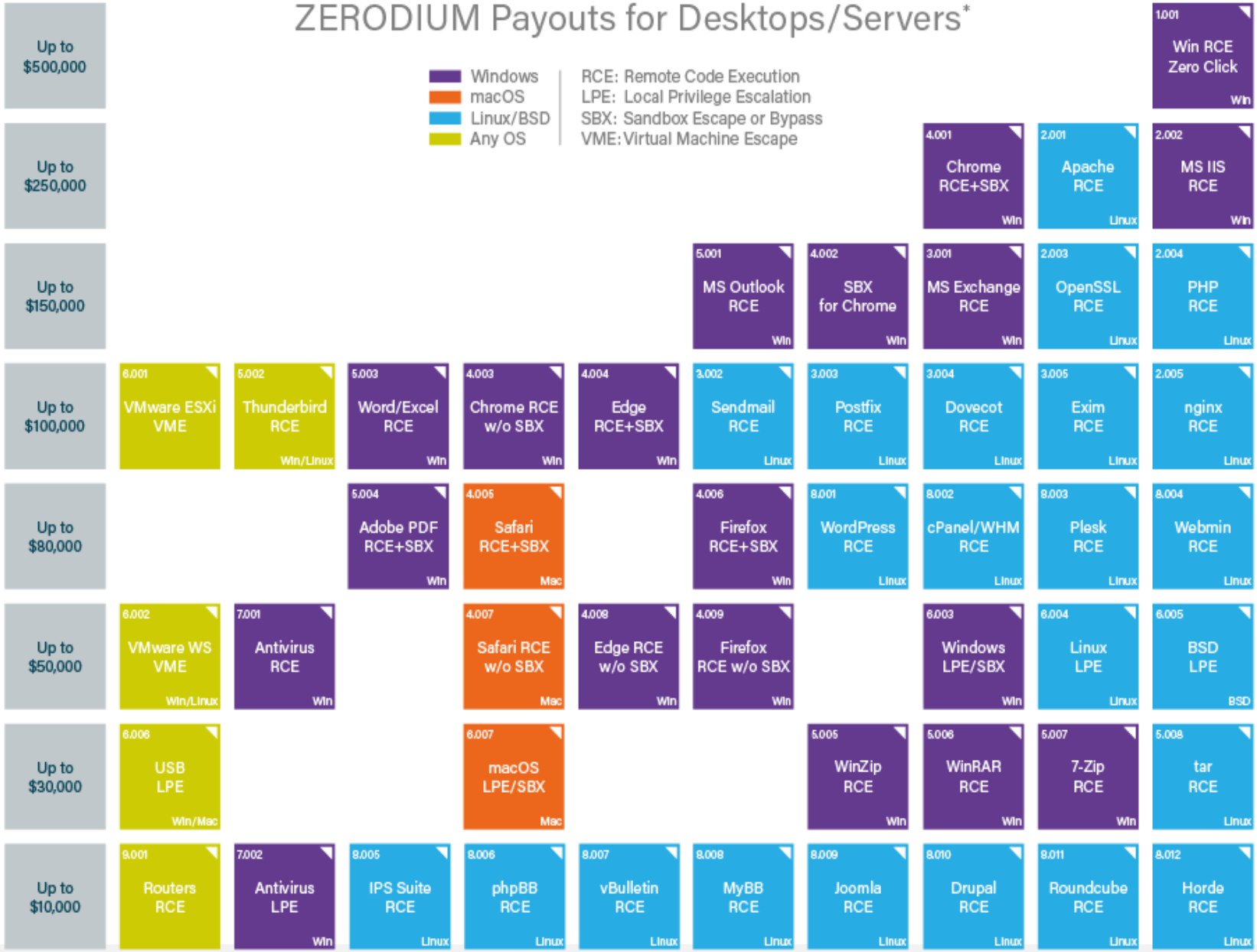
Divulgations de codes très sophistiqués



Somme de codes et techniques réutilisables

Aujourd'hui, les attaquants vont plus vite à réaliser de nouveaux codes d'exploitation que les défenseurs à mettre à jour leur système d'information

ZERODIUM Payouts for Desktops/Servers*



*All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.

ZERODIUM Payouts for Mobiles*

RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

iOS
Android
Any OS

Up to $1,500,000										1.001 iPhone RJB Zero Click iOS
Up to $1,000,000										1.002 iPhone RJB iOS
Up to $500,000	2.001 WeChat RCE+LPE iOS/Android	2.002 Viber RCE+LPE iOS/Android		2.003 FB Messenger RCE+LPE iOS/Android	2.004 Signal RCE+LPE iOS/Android	2.005 Telegram RCE+LPE iOS/Android	2.006 WhatsApp RCE+LPE iOS/Android	2.007 iMessage RCE+LPE iOS	2.008 SMS/MMS RCE+LPE iOS/Android	2.009 Email App RCE+LPE iOS/Android
Up to $200,000	3.001 Baseband RCE+LPE iOS/Android								4.001 Chrome RCE+SBX Android	4.002 Safari RCE+SBX iOS
Up to $100,000	5.001 Code Signing Bypass iOS	3.002 WiFi RCE+LPE iOS/Android		2.010 Media Files RCE iOS/Android	2.011 Documents RCE iOS/Android	6.001 LPE to Kernel iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $50,000	5.002 Code Signing Bypass Android	5.003 Secure Boot iOS	3.003 RCE via MitM iOS/Android					6.002 LPE to Root iOS/Android	4.007 Chrome UXSS/SOP iOS/Android	4.008 Safari UXSS/SOP iOS
Up to $25,000	5.004 TrustZone Android	5.005 Verified Boot Android			6.003 LPE to System Android	7.001 ASLR Bypass iOS/Android	7.002 kASLR Bypass iOS/Android	7.003 Seccomp Bypass Android	7.004 RKP Bypass Android	7.005 Knox Bypass Android
Up to $15,000	9.001 Information Disclosure iOS/Android							8.001 Passcode Bypass iOS	8.002 Touch ID Bypass iOS	8.003 PIN Bypass Android

Le cybercrime rentable

Fraude au président de 19,2M€ sur le Groupe Pathé

LE COURRIEL PIÉGÉ

Serveur de distribution

Envoi d'un courriel
Contenant une
pièce jointe piégé

Exemple de sujet de mail et/ou de nom de pièce-jointe :
Rapport mouvements militaire dans les Balkans

La victime clique sur la pièce jointe
permettant l'installation d'une porte dérobée

Attaquant

Annonce de la compromission

Prise de contrôle
De la machine
infectée

Victime

Serveur d'exfiltration

latéralisation de l'attaque

Exfiltration de
données sensibles

Eléments clés du réseau interne
(cœur de confiance AD, messagerie, serveur de fichier,
base de données…)

Réseau d'entreprise

Vers une sécurité du numérique

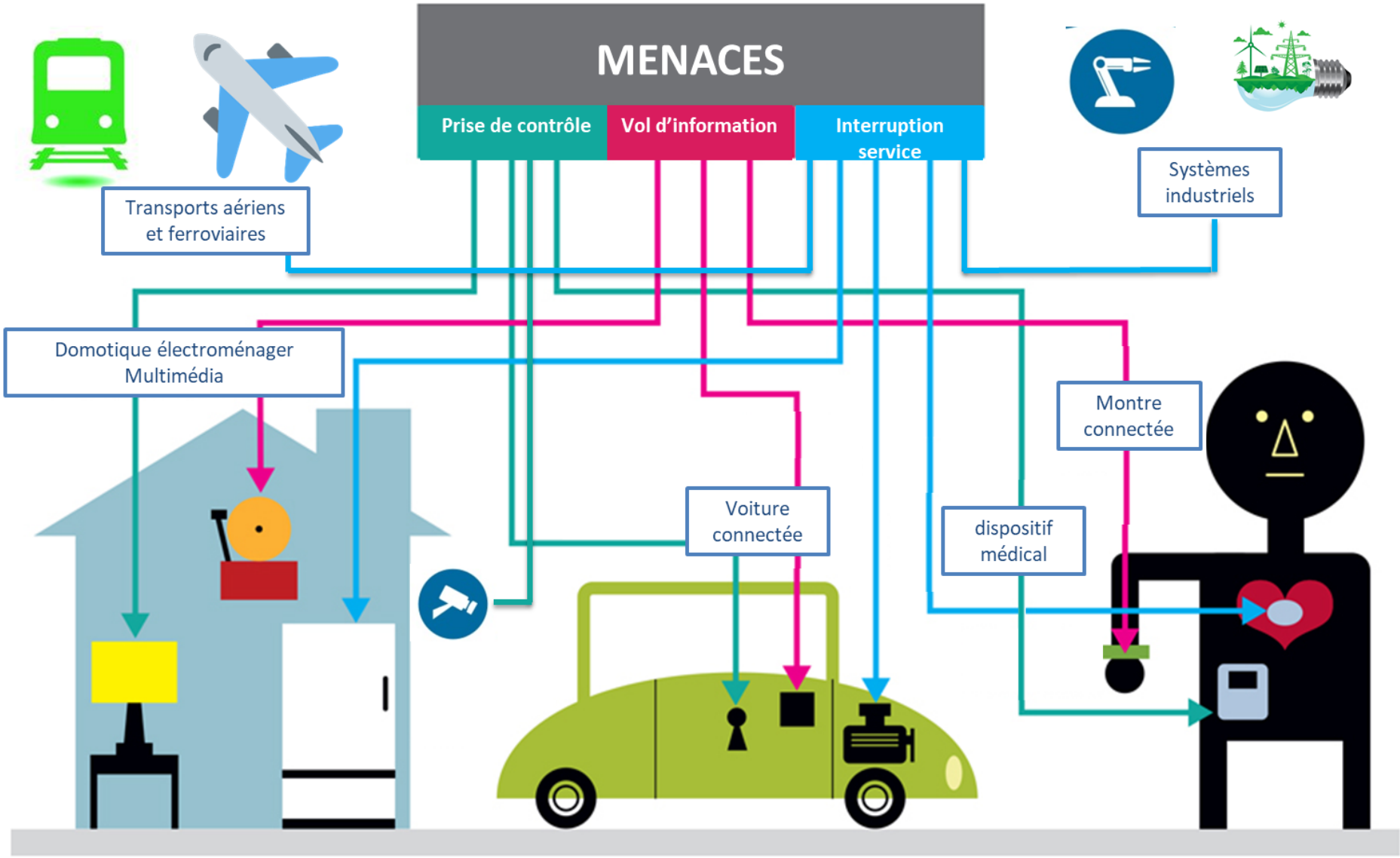


Illustration: J. D. King

Source : https://spectrum.ieee.org

Pourquoi les attaques réussissent-elles trop souvent ?

- **Sensibilisation et maturité insuffisante des utilisateurs**
- **Systèmes et applications pas à jour dont sites Web**
- **Politique de gestion des mots de passe insuffisante**
- **Pas de séparation des usages (utilisateur/administrateur) et des réseaux**
- Laxisme dans la gestion des droits d'accès
- Absence de surveillance des SI
- Cloisonnement insuffisant des systèmes (propagation latérale)
- Absence de restrictions (périphériques…)
- Nomadisme / télétravail incontrôlés

S’emparer de la question de la sécurité numérique

5 questions d’un dirigeant pour faire le point

- Depuis quand n’ai-je pas entendu parler de cyber sécurité?
- Mon entreprise est-elle une cible d’intérêt pour des attaquants?
- Ai-je pris toutes les précautions pour protéger mes informations et les échanges avec mes partenaires et mes collaborateurs?
- Quel est la part du budget consacrée à la sécurité informatique?
- Ai-je déjà parlé de cyber sécurité à mes collaborateurs?

S’emparer de la question de la sécurité numérique

5 questions à poser à mon RSSI ou info-gérant

- Quelles sont nos principales vulnérabilités?
- Quels sont les moyens de protection actuellement en place pour lutter contre les attaques et codes malveillants?
- A-t-on déjà fait un audit de sécurité des SI? Une analyse de risques? Une cartographie des SI?
- Sommes-nous préparés si une crise d’origine cyber survenait?
- Disposons-nous d’une couverture juridique et nos contrats d’assurance intègrent-ils le risque cyber?

TABLE DES MATIERES

Pour aller plus loin - www.ssi.gouv.fr

https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/

https://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/

https://www.ssi.gouv.fr/entreprise/guide/guide-delaboration-dune-charte-dutilisation-des-moyens-informatiques-et-des-outils-numeriques/

www.secnumacademie.gouv.fr

www.cybermalveillance.gouv.fr

Informer - Sensibiliser