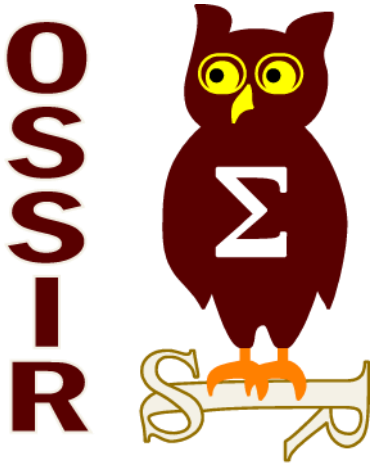


Revue d'actualité

OSSIR Résist – Janvier 2013

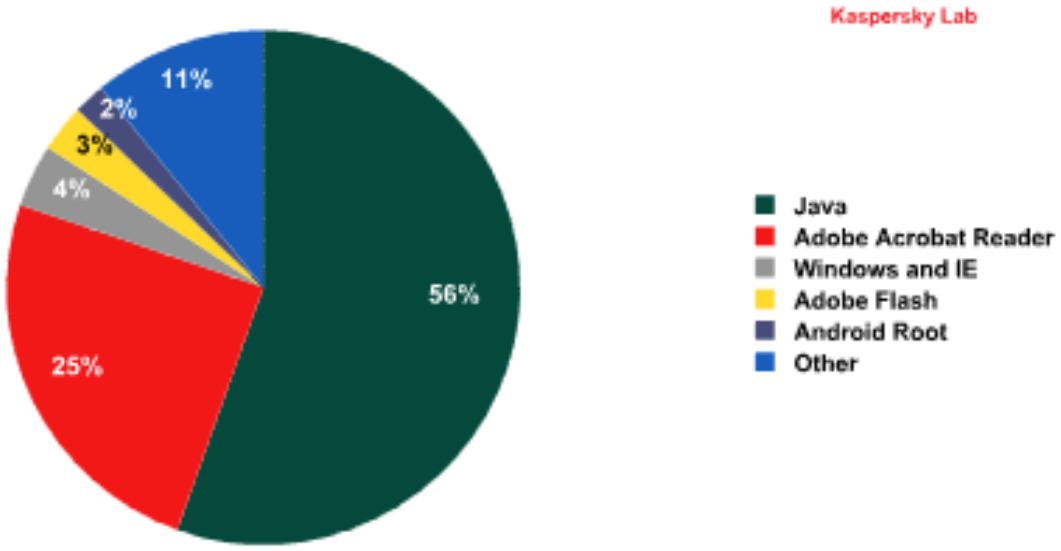
Presented by
Etienne Maynier

MDAL
WE PROTECT YOUR ASSETS

Evolution des menaces (1/3)

- Internet Explorer, Adobe Reader et Java toujours en tête

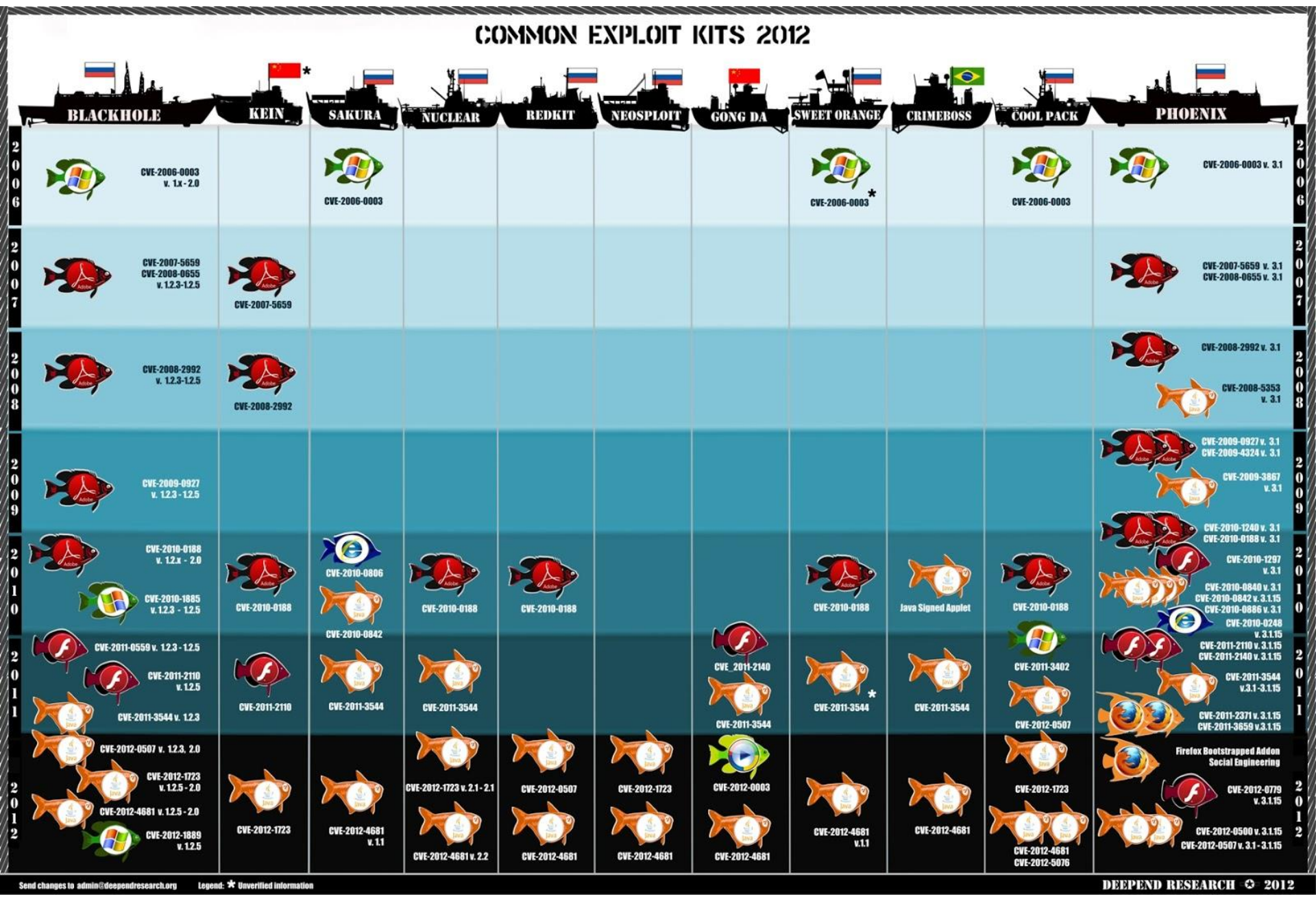
- Internet Explorer vulnérable à des 0day exploitées dans la nature pendant 89 jours au cours des 19 derniers mois
  - http://krebsonsecurity.com/2012/10/in-a-zero-day-world-its-active-attacks-that-matter/



http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012

Evolution des menaces (2/3)

- Un chercheur trouve une faille dans Java SE en Octobre, Oracle attend jusqu'au patch de février…
  - https://threatpost.com/en_us/blogs/oracle-leaves-fix-java-se-zero-day-until-february-patch-update-101712
- Suppression de Java par Apple
  - http://www.lemonde.fr/technologies/article/2012/10/22/apple-supprime-java-de-ses-navigateurs_1778850_651865.html
- Nouvelle 0day découverte en Janvier
  - http://www.theinquirer.net/inquirer/news/2235878/security-vendors-warn-users-to-disable-java-after-zero-day-exploit-is-found
- Arrêtons Java dans le navigateur !



http://www.deependresearch.org/2012/11/common-exploit-kits-2012-poster.html

Etudes

- Service Sells Access to Fortune 500 Firms
  - Un serveur chez Cisco pour $4,55 !
  - http://krebsonsecurity.com/2012/10/service-sells-access-to-fortune-500-firms/

- Sophail 2
  - XSS, buffer overflows…
    - *"Sophos were able to convince me they were working with good intentions, but they were clearly ill-equipped to handle the output of one co-operative security researcher working in his spare time."*
    - *http://seclists.org/fulldisclosure/2012/Nov/31*

Incidents

- En mai 2012, infiltration sur le réseau de l'Elysée
  - Par les USA ?
    - http://lexpansion.lexpress.fr/high-tech/cyberguerre-comment-les-americains-ont-pirate-l-elysee_361225.html
- Turktrust : émission d'un certificat pour *.google.com
  - Un autre exemple des problèmes de SSL
  - http://krebsonsecurity.com/2013/01/turkish-registrar-enabled-phishers-to-spoof-google/
- 4,5 millions de routeurs compromis au Brésil via une CSRF
  - http://www.h-online.com/security/news/item/4-5-million-routers-hacked-1722430.html
- Red October : nouvelle campagne type APT
  - Cible principalement l'Europe de l'Est, la Russie et l'Asie
  - Notez la recherche de fichiers Acid Cryptofiler…
  - http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

Huawei & ZTE

- Suite du bras de fer avec les sociétés chinoises

- Les USA designed Huawei et ZTE commes « menaces pour la sécurité nationale »
  - http://www.theinquirer.net/inquirer/news/2215286/us-house-calls-huawei-and-zte-threats-to-national-security
  - Suivi par le Canada
    - http://www.theinquirer.net/inquirer/news/2215917/canada-hints-that-it-will-lock-huawei-out-of-network-talks
  - Huawei offre l'accès à son code source au gouvernement Australien
    - http://www.bbc.co.uk/news/business-20053511

- HITB : *"I don't know if there are backdoors - but it doesn't matter since there are so many vulnerabilities."*
  - http://www.zdnet.com/hack-in-the-box-researcher-reveals-ease-of-huawei-router-access-7000005600/
  - Huawei envoi une équipe collaborer avec les chercheurs à grand renfort de communication
    - http://www.h-online.com/security/news/item/Huawei-sends-team-to-visit-critical-researcher-1741575.html

Cryptographie

- Fin de la compétition SHA3 : Keccak 1 a gagné
  - Vraiment utile ?
  - http://csrc.nist.gov/groups/ST/hash/sha-3/winner_sha-3.html

- On pourrait voir des attaques réelles sur SHA1 dès 2018
  - https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html

Veille légale

- Retour du projet de « secret des affaires »
  - http://www.lemonde.fr/economie/article/2012/10/06/contre-l-espionnage-industriel-bercy-relance-l-idee-d-instituer-un-secret-des-affaires_1771215_3234.html

- Cour de justice européenne : les fonctionnalités d'un logiciels ne sont pas protégées par le droit d'auteur
  - Autorise le reverse engineering ?
  - http://pro.01net.com/editorial/577457/le-reverse-engineering-autorise-par-la-cour-de-justice-europeenne/

- Une commissaire européenne plaide pour une obligation de notification lors d'un incident de sécurité
  - http://www.01net.com/editorial/580905/l-europe-veut-que-les-entreprises-signalent-leurs-cyberattaques

Sujets du jour

- *L'analyse de logs*
  - Sébastien Tricaud - Honeynet.org

- *Retour d'expérience sur une campagne de phishing*
  - Fabrice Prigent - Université Toulouse 1 Capitole