

# Revue d'actualité

OSSIR Résist – Janvier 2013

Presented by  
Etienne Maynier

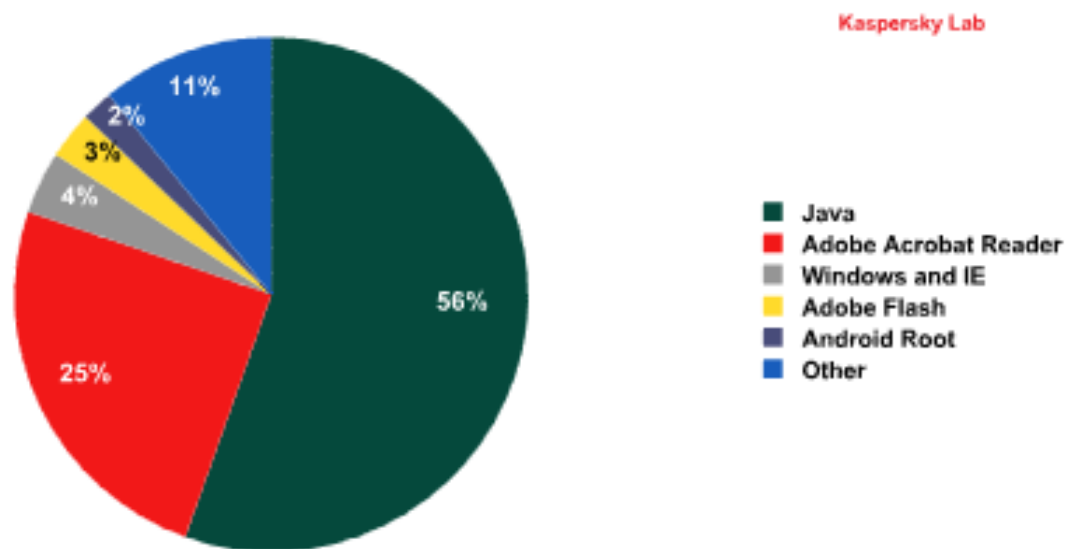


**MDAL**  
WE PROTECT YOUR ASSETS



# 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](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](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](http://www.lemonde.fr/technologies/article/2012/10/22/apple-supprime-java-de-ses-navigateurs_1778850_651865.html)
- Nouvelle Oday 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 !

# COMMON EXPLOIT KITS 2012

	BLACKHOLE	KEIN	SAKURA	NUCLEAR	REDKIT	NEOSPLOIT	GONG DA	SWEET ORANGE	CRIMEBOSS	COOL PACK	PHOENIX
2006	 CVE-2006-0003 v. 1.x - 2.0		 CVE-2006-0003					 CVE-2006-0003 *		 CVE-2006-0003	 CVE-2006-0003 v. 3.1
2007	 CVE-2007-5659 CVE-2008-0655 v. 1.2.3-1.2.5	 CVE-2007-5659									 CVE-2007-5659 v. 3.1 CVE-2008-0655 v. 3.1
2008	 CVE-2008-2992 v. 1.2.3-1.2.5	 CVE-2008-2992									 CVE-2008-2992 v. 3.1  CVE-2008-5353 v. 3.1
2009	 CVE-2009-0927 v. 1.2.3 - 1.2.5										 CVE-2009-0927 v. 3.1 CVE-2009-4324 v. 3.1  CVE-2009-3867 v. 3.1
2010	 CVE-2010-0188 v. 1.2.x - 2.0  CVE-2010-1885 v. 1.2.3 - 1.2.5	 CVE-2010-0188	 CVE-2010-0806  CVE-2010-0842	 CVE-2010-0188	 CVE-2010-0188			 CVE-2010-0188	Java Signed Applet	 CVE-2010-0188	 CVE-2010-1240 v. 3.1 CVE-2010-0188 v. 3.1  CVE-2010-1297 v. 3.1  CVE-2010-0840 v. 3.1 CVE-2010-0842 v. 3.1.15 CVE-2010-0886 v. 3.1  CVE-2010-0248 v. 3.1.15
2011	 CVE-2011-0559 v. 1.2.3 - 1.2.5  CVE-2011-2110 v. 1.2.5	 CVE-2011-2110	 CVE-2011-3544	 CVE-2011-3544	 CVE-2011-3544		 CVE-2011-2140	 CVE-2011-3544 *	 CVE-2011-3544	 CVE-2011-3402	 CVE-2011-2110 v. 3.1.15 CVE-2011-2140 v. 3.1.15  CVE-2011-3544 v.3.1-3.1.15
2012	 CVE-2012-0507 v. 1.2.3, 2.0  CVE-2012-1723 v. 1.2.5 - 2.0  CVE-2012-4681 v. 1.2.5 - 2.0  CVE-2012-1889 v. 1.2.5	 CVE-2012-1723	 CVE-2012-4681 v. 1.1	 CVE-2012-1723 v. 2.1 - 2.1  CVE-2012-4681 v. 2.2	 CVE-2012-0507  CVE-2012-4681	 CVE-2012-1723  CVE-2012-4681	 CVE-2012-1723  CVE-2012-0003  CVE-2012-4681	 CVE-2012-4681 v.1.1	 CVE-2012-4681	 CVE-2012-1723  CVE-2012-4681 CVE-2012-5076	 CVE-2012-1723  CVE-2012-4681  CVE-2012-0507 v. 3.1-3.1.15 Firefox Bootstrapped Addon Social Engineering  CVE-2012-0779 v. 3.1.15

Send changes to [admin@deependresearch.org](mailto:admin@deependresearch.org) Legend: \* Unverified Information

DEEPEND RESEARCH © 2012



# 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'Élysée
  - Par les USA ?
    - [http://lexpansion.lexpress.fr/high-tech/cyberguerre-comment-les-americains-ont-pirate-l-elysee\\_361225.html](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](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](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](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](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 - Honey.net.org
  
- *Retour d'expérience sur une campagne de phishing*
  - Fabrice Prigent - Université Toulouse 1 Capitole



© MDAL SARM. All rights reserved. Confidential and proprietary document. This document and all information contained herein is the sole property of MDAL SARM. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of MDAL SARM. This document and its content shall not be used for any purpose other than that for which it is supplied. The statements made herein do not constitute an offer. They are based on the mentioned assumptions and are expressed in good faith. Where the supporting grounds for these statements are not shown, MDAL SARM will be pleased to explain the basis thereof.