DANS LE SECRET DES FAILLES INFORMATIQUES

LE 3 SEPTEMBRE 2012 ***PIERRE ALONSO***

Le business des *Zero Day* est des plus opaques. Des *Zero Day* ? Ce sont les failles de sécurité dont l'existence n'a pas été encore révélées et se vendent dès lors à prix d'or, comme le raconte le *Washington Post*. Un marché dans lequel une boite française, Vupen, tient une bonne place. Non sans s'attirer de nombreuses critiques.

Au profane, *Zero Day* ne dira rien. Un titre de film ou de roman d'espionnage tout au plus. L'expression est bien connue des experts en sécurité informatique, source d'adrénaline ou de sueurs froides. Un *Zero Day* désigne une faille encore inconnue dans un logiciel. Stuxnet, le virus **fabriqué par les États-Unis et Israël** pour saboter le programme nucléaire iranien, s'est appuyé sur au moins quatre failles de ce type.

Le *Washington Post* a plongé dans l'univers feutré et méconnu du marché de ces failles, entre acheteurs privés et publics et vendeurs de tous horizons. *"Tout le monde en veut"* a déclaré Chris Soghoian, un chercheur en sécurité informatique basé à Washington. Mais le fructueux business reste secret. Qui achète, qui vend ? La plupart des entreprises affirment limiter les ventes de failles à des agences de renseignement ou à des sous-traitants de l'armée.

60 000 dollars la faille

Une boite française, **Vupen**, est parvenue à se faire une réputation dans ce milieu interlope. En janvier 2012, une équipe de cinq experts de l'entreprise – dont le co-fondateur Chaouki Bekrar – **avait découvert** l'une de ces failles dans le navigateur Google Chrome au ***Pwn2Own Contest***. Récompense pour la découverte : 60 000 dollars. Une autre découverte pour la même compétition n'a pas été rendue publique par Vupen qui a préféré la garder pour ses clients. Hors compétitions officielles, les chiffres donnent le tournis, *"parfois des centaines de milliers de dollars la faille"* selon le quotidien américain.

La très grande discrétion de Vupen lui a valu de vertes critiques. Irresponsable, coupable de donner une mauvaise réputation à l'ensemble des acteurs du marché… Chaouki Bekrar s'en est défendu auprès du *Washington Post*, affirmant ne vendre qu'*"aux agences de renseignement des pays membre de l'OTAN"*, en écho à **la présentation officielle** de Vupen sur son site.

D'autres entreprises se disent plus scrupuleuses, comme l'américaine **Netragard**, qui affirme ne vendre qu'à ses alter-ego américains et seulement en connaissant l'utilisation finale. Charlie Miller, consultant dans le privé après une carrière à la NSA invoque une équation insoluble pour les découvreurs de *Zero Day* :

> ***Dois-je faire ce qui est bon pour la plupart des gens et ne pas toucher d'argent du tout, ou dois-je vendre au gouvernement américaine et gagner 50 000 dollars ?***

L'Allemagne a tranché, avec fermeté : le commerce de *Zero Day* est interdit, de même que leur publication sans rémunération et même le simple fait de les chercher. Au États-Unis, il reviendra au département du Commerce de décider du sort de ces précieuses failleurs, notamment pour l'exportation.

Le *Washington Post* a consacré une série d'articles sur les *Zero Day*, à retrouver **en suivant ce lien**.

Illustration photo CC by-nc-nd **ANTPhotos**

Mise à jour le 3 septembre à 19h45 : correction d'une coquille sur une occurence du nom de Chaouki Bekrar.

PRFIRMIN
le 3 septembre 2012 - 17:10 • SIGNALER UN ABUS - PERMALINK

"L'Allemagne a tranché, avec fermeté : le commerce de Zero Day est interdit, de même que leur publication sans rémunération et même le simple fait de les chercher."

Autrement dit ceux qui soumettent des rapports de faille sont de dangereux criminel. La mesure type votée par de vieux croûtons qui ne comprennent pas la portée du problème…

VOUS AIMEZ 8 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GASCHE
le 3 septembre 2012 - 17:36 • SIGNALER UN ABUS - PERMALINK

"L'Allemagne a tranché, avec fermeté : le commerce de Zero Day est interdit, de même que leur publication sans rémunération et même le simple fait de les chercher."

Dit comme ça, ça n'a aucun sens, j'ai du mal à croire à une loi interdisant de chercher des failles dans ses applications. Je suppose qu'il s'agit d'une erreur de formulation. Pourriez-vous fournir la source de ce commentaire ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PIERRE ALONSO
le 3 septembre 2012 - 17:43 • SIGNALER UN ABUS - PERMALINK

Bonjour Gasche,

Comme indiqué dès le début, la source de cet article est une enquête parue dans le Washington Post. Le passage que vous mettez en exergue est une reprise de cet extrait :

"Germany, meanwhile, is one of the few countries to stringently regulate exploits. Not only is it illegal to sell exploits in Germany, but it is also illegal to distribute them for free — a practice used to notify the world of vulnerabilities — or ***to create or research them*** *."*

J'espère répondre à votre question,
Cordialement

PA

VOUS AIMEZ 2 VOUS N'AIMEZ PAS 0 LUI REPONDRE

NICOLAS
le 4 septembre 2012 - 10:27 • SIGNALER UN ABUS - PERMALINK

Cela parait délirant. Dans le logiciel libre, une personne qui trouve un bug, le remonte le plus vite possible aux auteurs. C'est le principe du logiciel libre : le test est hautement parallélisable. Ce genre de loi rendrait impossible la remonté d'erreur lié à la sécurité ? Cela parait vraiment énorme.

VOUS AIMEZ 4 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LEGUMX
le 3 septembre 2012 - 18:41 • SIGNALER UN ABUS - PERMALINK

Alors, dans ce cas là, faire des rapports d'exploits pour la communauté afin de pouvoir fixer les failles
et vendre des exploits à des sociétés pour un prix d'or sont considérés de la même manière par le droit allemand ?
C'est complètement débile…
Après qu'on soit passé par des cas extrêmes comme ce qui s'est passé par exemple avec zataz et d'autres, on ne fait toujours pas de distinction ?

VOUS AIMEZ 9 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

Failles, éthique et supermarchés « Hacker Area …….. ……..Territoire Hacker le 4 septembre 2012 - 13:29

[...] Polémiques autour des pratiques commerciales entourant les 0Day (parution postérieure à cet artic… Share this:TwitterFacebookJ'aime ceci:J'aimeSoyez le premier à aimer ceci. Tags:0day, bug, Hackito Ergo Sum 2010, virtualisation, vulnérabilité Comments RSS feed [...]