La politique biaisée de divulgation des zero day de la NSA

Avec les documents d'Edward Snowden et les différentes accusations d'utiliser des failles critiques pour mener à bien des opérations souterraines, les agences américaines de renseignement obligent le gouvernement à montrer un peu de transparence. C'est ce qui vient de se produire avec une infographie de la NSA (Nation Security Agency) censée démontrer sa politique de divulgation de failles zero day.

Le chiffre est annoncé en gros pour qu'il imprègne bien le cerveau : 91%. La NSA partage donc une majorité des vulnérabilités critiques découvertes avec les éditeurs pour les corriger. Cette version est selon Reuters qu'une partie émergée de l'iceberg. En effet, l'infographie ne dit pas quand ces découvertes sont partagées. Or selon d'anciens responsables du gouvernement américain, l'agence de sécurité utilise en général ces zero day achetées à l'extérieur pour mener ses propres opérations offensives et ne communique qu'après leurs découvertes aux éditeurs, dans un laps de temps qui n'est pas précisé. Le chiffre de 91% est donc à prendre avec toutes les précautions d'usage.

Idem pour les 9% restant, la NSA explique qu'il s'agit entre autres de vulnérabilités corrigées avant publication. Mais, ce pourcentage intègre aussi des zero day qui ne seront pas communiqués pour des raisons de sécurité nationale. Parmi ces failles qui ont été découvertes par la suite, on peut citer Stuxnet qui avait pour objectif de saboter le programme iranien de centrifugeuse nucléaire pour l'enrichissement de l'uranium.

Un marché nébuleux, mais actif

Derrière cette présentation se profile surtout le marché des failles critiques qui est en pleine ébullition. Un véritable écosystème s'est constitué autour de ce marché. En première ligne, il y a les chercheurs capables de trouver, dénicher un zero day. Ils sont de tous horizons, universitaires, salariés d'une grande entreprise, etc. Mais plusieurs sociétés se sont spécialisées dans ce domaine comme Vupen, Hacking Team (devenu médiatique à cause de son piratage) ou plus récemment Zerodium qui a versé 1 million de dollars à une équipe de hacker pour la découverte d'une brèche dans iOS 9.

Autour de ces chercheurs et ces sociétés gravitent les Etats, les cybercriminels et les éditeurs. Les Etats et la NSA en tête sont vite de devenus des acheteurs en puissance de failles zero day. Mais les cybercriminels ne sont pas en reste et proposent des sommes alléchantes pour récupérer des talents dans ce domaine. Enfin les éditeurs tentent de tirer leur épingle du jeu en multipliant les programmes de chasse aux bugs avec des primes de plus en plus élevées. Et ce marché n'est pas prêt de se tarir, à la dernière

THE NATIONAL SECURITY AGENCY

Discovering IT Problems, Developing Solutions, Sharing Expertise

Q: When the U.S. Government learns of vulnerabilities in information-technology products, will it disclose information about those vulnerabilities?

A: **The U.S. Government takes seriously its commitment to an open and interoperable, secure, and reliable Internet. In the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. We all rely on the Internet and connected systems for much of our daily lives. Plus, our economy would not function without them. For these reasons, disclosing vulnerabilities usually makes sense. But there are legitimate pros and cons to the decision to disclose vulnerabilities, and the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences.**

The National Security Council has an interagency process to consider when to disclose vulnerabilities. The process requires the government to weigh many factors, including the importance of the information to the nation's security. While these decisions can be complex,

THE GOVERNMENT'S BIAS IS TO RESPONSIBLY AND DISCREETLY DISCLOSE VULNERABILITIES.

For many years prior to the establishment of the interagency process, NSA had an internal review process in this area. NSA's review continues and now informs the interagency process. Historically, NSA has released more than

91

PERCENT OF VULNERABILITIES DISCOVERED IN PRODUCTS THAT HAVE GONE THROUGH OUR INTERNAL REVIEW PROCESS AND THAT ARE MADE OR USED IN THE UNITED STATES.

The remaining 9% were either fixed by vendors before we notified them or not disclosed for national security reasons.

DISCLOSING A VULNERABILITY CAN MEAN THAT WE FORGO AN OPPORTUNITY TO:

- Collect crucial foreign intelligence that could thwart a terrorist attack.
- Stop the theft of our nation's intellectual property.
- Discover even more dangerous vulnerabilities that are being used to exploit our networks.

THE **MEN** AND **WOMEN** OF NSA **MAKE A DIFFERENCE.**

For more than 60 years, the National Security Agency has worked to ensure that appropriate security solutions are in place to protect our critical infrastructure, national security systems, and the information on those systems. NSA's Information Assurance Directorate pioneered what is now called cybersecurity. We make information and information technology an asset for the United States – and a liability for its adversaries.

Learn more at www.nsa.gov/ia

A lire aussi :

Dix failles zero day dévoilées en septembre

Des failles zero day trouvées chez Kaspersky et FireEye

Crédit Photo : Batofolux-Shutterstock