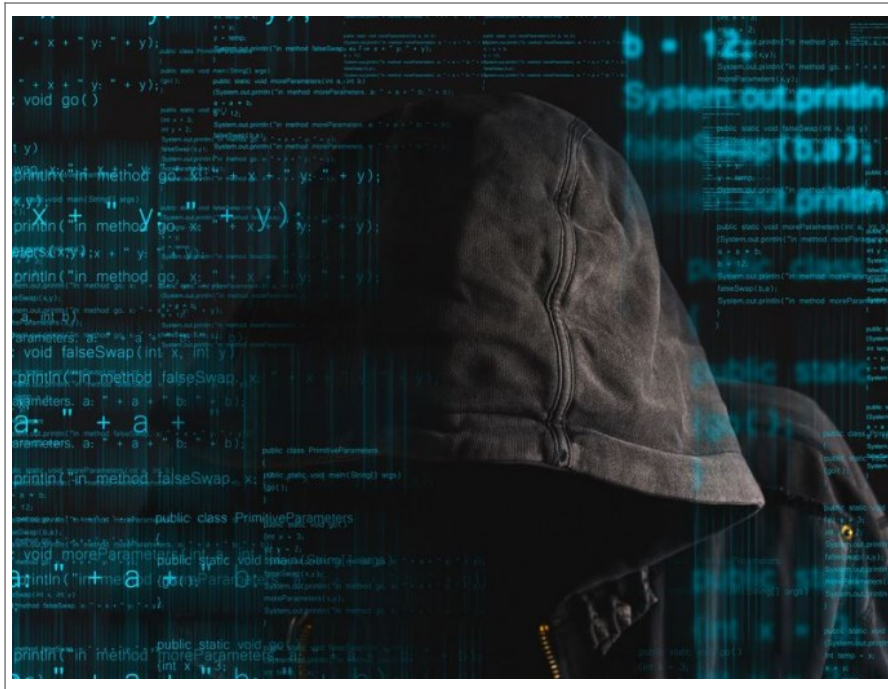


Shadow Brokers, une affaire de Cyberespionnage



Shadow Brokers,
une affaire de
Cyberespionnage

1) Pourquoi un tel intérêt pour les Shadow Brokers ?

2) Le hacking de la NSA est-il établi ?

3) Que dit cette affaire du groupe Equation ?

4) Que renferme l'archive des Shadow Brokers ?

Plusieurs chcheurs en sécurité se sont déjà penchés sur le cyber-arsenal mis à disposition par les Shadow Brokers (lire notamment l'analyse de Mustafa Al-Bassam ou la synthèse réalisée par Softpedia). On y trouve des exploits, autrement dit des codes d'exploitation permettant de prendre le contrôle ou d'espionner des pare-feu ou passerelles VPN fournis par de grands constructeurs comme Cisco, Juniper ou Fortinet. Des constructeurs qui ont déjà reconnu que les outils mis en ligne menaçaient bien certains de leurs matériels. Mais, dans tous les cas, il s'agit de générations anciennes de machines. Les appliances Cisco Pix, ciblées par plusieurs outils, ne sont par exemple plus supportées par le constructeur depuis 2009. [lire la suite]

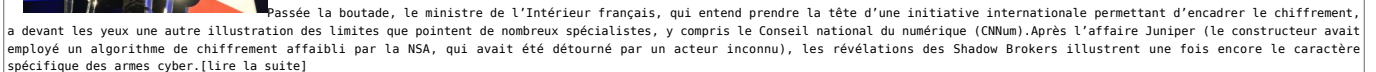
Et il y a aussi les outils dont la vocation ne s'inscrivent pas à cibler une gamme de machines en particulier. *The Intercept* explique ainsi que des éléments d'une architecture exploitée par la NSA pour mettre en place des attaques de type Man-in-the-Middle, autorisant l'interception de requêtes Web, figurent dans l'archive des Shadow Brokers. Sans risque de se tromper, la réponse est non. « Comme il y a 300 Mo de code, de documentations, de binaires, personne n'a publié d'analyse complète », remarquent Hervé Schauer et Christophe Renard. [lire la suite]

Voir de tels outils mis à la disposition de cybercriminels est évidemment inquiétant. « On est ici face à des outils d'attaque de haut niveau, mis librement à disposition sur le Web, explique Jérôme Billois. Les entreprises doivent donc être très attentives, effectuer l'inventaire des matériels exposés sur leur parc et apporter les modifications nécessaires pour protéger leurs infrastructures. Heureusement, les exploits mis au jour sont assez anciens et ciblent donc du matériel âgé. Mais certaines machines peuvent toujours être en exploitation. » Au fur et à mesure que les codes de l'archive des Shadow Brokers seront décryptés, des correctifs et des indicateurs de compromission vont être publiés. Ce qui permettra aux RSSI de contrer la menace. C'est donc plutôt une course de fond qui s'engage. [lire la suite]

La liste des suspects s'est très vite limitée quelques noms. Très rapidement, Nicolas Weaver, de l'université de Berkeley, pointe la Chine, soupçonnée de nombreux actes de cyber-espionnage contre les intérêts américains, et la Russie. Une seconde hypothèse que défend lui aussi Edward Snowden, précisément réfugié en Russie après avoir été à l'origine de la plus importante fuite de données de l'histoire de la NSA. [lire la suite]

9) Quelles sont les conséquences possibles ?

10) Qu'en pense Bernard Cazeneuve ?



Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en
Protection des Données Personnelles

Réagissez à cet article

Original de l'article mis en page : Cyberespionnage : 10 questions pour comprendre l'affaire Shadow Brokers