elastic security labs

Les 10 grandes leçons que les directeurs de la sécurité de l'information doivent retenir du rapport 2023 sur les menaces mondiales

Conçu pour fournir des informations exploitables sur les menaces, le second rapport annuel d'Elastic sur les menaces mondiales présente les principales conclusions tirées après plusieurs mois d'analyse de plus de 1 milliard de points de données, obtenus grâce à des systèmes de télémétrie privés et publics. Elastic Security Labs a réparti ces informations exploitables en trois grandes catégories, à savoir les prévisions concernant les menaces, les tactiques des utilisateurs malveillants et les systèmes.

Prévisions concernant les menaces

1. **Les outils open source vont gagner en popularité.** Les outils open source représentent pour les utilisateurs malveillants une entrée gratuite et facile dans la cybercriminalité. Dans le cadre de l'analyse menée pour rédiger son rapport sur les menaces mondiales et lors de recherches préalables aux résultats présentés ici, Elastic a observé plusieurs outils de malware open source, comme le rootkit r77 et JOKERSPY.

2. **Le nombre de malwares en tant que service (MaaS) destinés aux utilisateurs malveillants novices va augmenter.** Les utilisateurs malveillants ont recours au modèle "en tant que service" (AaS) afin de combler leurs lacunes en matière de produits et de connaissances, comme le prouve la popularité des RaaS. Les prestataires de solutions AaS malveillantes vont diversifier leurs portefeuilles afin de mieux servir les acheteurs. En outre, les utilisateurs malveillants qui ont recours aux MaaS se reposeront sur les *techniques de brouillage et de masquage*.

3. **Les utilisateurs malveillants vont davantage manipuler les environnements au lieu de se cacher.** Alors que les environnements sont de plus en plus résistants aux attaques, les utilisateurs malveillants tentent de plus en plus souvent de désactiver les capteurs de sécurité ou de les trafiquer d'une manière ou d'une autre. Outre l'analyse réalisée pour rédiger son rapport sur les menaces mondiales, Elastic a observé une hausse des attaques exploitant les défauts de conception des systèmes d'exploitation, comme BYOVD (Bring Your Own Vulnerable Driver), pour déployer un pilote doté d'une ou de plusieurs faiblesses exploitables.

Tactiques des utilisateurs malveillants

4. **Les ransomwares s'étendent et se diversifient.** Avec des exemples de grande envergure, comme WannaCry et NotPetya, les ransomwares sont devenus une grave menace au fil des ans. Les campagnes de ransomwares en tant que service (RaaS) représentent 81 % de l'ensemble des ransomwares observés, probablement car les utilisateurs malveillants novices comme chevronnés doivent franchir un obstacle moins difficile pour accéder à un système. Selon nos prévisions, les utilisateurs malveillants vont innover davantage à l'avenir dans ce domaine.

5. Les utilisateurs malveillants se déplacent facilement dans les systèmes.
Quasiment la moitié (soit 43,89 %) des comportements observés des points de terminaison concerne une technique d'*Évasion par la défense*. Comme le suggère l'importance de ce nombre, les utilisateurs malveillants savent comment passer outre les systèmes de sécurité et le font en toute simplicité.

6. Du code malveillant est exécuté via les utilitaires intégrés des systèmes d'exploitation.
D'après les observations d'Elastic, 48 % des techniques d'*Évasion par la défense* s'exécutant sur des points de terminaison étaient des *méthodes d'exécution de proxy binaire*, ce qui permet aux utilisateurs malveillants d'exécuter du code malveillant dans le cadre d'un programme de système d'exploitation natif. La popularité de cette tactique peut s'expliquer par le caractère chronophage de l'analyse de ces types d'alertes.

7. Les utilisateurs malveillants utilisent des techniques *d'Accès aux identifiants* dans les environnements cloud.
Elastic a observé une hausse de 11 % des signaux d'*Accès aux identifiants*, une preuve que les identifiants sont devenus une composante fondamentale du processus d'intrusion dans le cloud. Cette observation pourrait également indiquer qu'il est facile de collecter des identifiants ou sous-entendre que les environnements ne bénéficient pas de la visibilité nécessaire pour repérer les utilisations frauduleuses d'identifiants valides.

Systèmes

8. L'amélioration de l'observabilité sous Windows a révélé la popularité d'Azure.
La visibilité d'Elastic dans les environnements Windows s'est améliorée cette année : elle a augmenté de 422 % depuis l'analyse de l'année dernière qui tenait compte de la nouvelle visibilité dans Microsoft 365. Dans le cadre de notre analyse des prestataires de services cloud, nous avons observé une hausse de l'activité d'Azure, qui est passée de 13,14 % l'année dernière à 36 % en 2023. Même si la majorité des signaux concerne AWS, ceux provenant des environnements AWS ont diminué d'environ 10 %.

9. Alors que la majorité des signaux de points de terminaison survient sous Windows, les signaux de macOS et de Linux ont augmenté de manière notable.
Sur la totalité des alertes liées aux comportements des points de terminaison, 94 % ciblaient des systèmes Windows, notamment à cause de la hausse des données télémétriques consacrées spécialement à ce système d'exploitation. Elastic a constaté d'importantes augmentations générales des signaux pour Windows, Linux, et macOS. Avec une hausse de 118 %, les innovations concernant macOS ont mis en lumière de nouvelles découvertes, comme RUSTBUCKET.

10. La plupart des infections par malwares observées ont touché des systèmes Linux.
Malgré l'observabilité renforcée dans l'ensemble des systèmes grâce à Elastic, 91,2 % des infections observées ont eu lieu sur Linux. En particulier, la plupart d'entre elles impliquaient une intervention non humaine. Il s'agissait d'attaques automatisées et éventuellement arbitraires.

Maîtrise des menaces

Préparez-vous à l'évolution de ces menaces et à d'autres changements. Découvrez les suggestions des spécialistes d'Elastic Security Labs en lisant le rapport 2023 d'Elastic sur les menaces mondiales. Suivez Elastic Security Labs sur X, ex-Twitter, (@ElasticSecLabs) et lisez nos articles afin de connaître les dernières nouveautés en matière de menaces, recherches et autres.

