

Cyber Crucible teste-t-il de manière exhaustive tous les rançongiciels possibles ?

Cyber Crucible fonctionne à partir d'une modélisation comportementale au niveau du noyau, afin de découvrir très rapidement les comportements de vol de données, de vol d'identifiants et de chiffrement par rançongiciel. Les décisions comportementales sont prises à partir d'informations issues du comportement des processus, de comportements dérivés de la mémoire, et de certains types de comportements issus de fichiers, afin de prendre une décision au moment même où l'extorsion est sur le point de se produire.

Malgré le très grand nombre d'échantillons de logiciels de rançongiciel et d'extorsion, ceux-ci peuvent être classés, sur le plan comportemental, en un nombre relativement restreint d'ensembles.

En surface, cependant, les défenses « superficielles » utilisées par une variété d'outils de sécurité doivent contrer un très grand nombre d'outils d'extorsion. Il est important de comprendre que nos analyses comportementales vont beaucoup plus en profondeur dans les outils et les méthodes des attaquants, ce qui réduit considérablement le besoin d'un type de test (impossible) exhaustif de tous les logiciels malveillants possibles, en permanence.

Les développeurs de Cyber Crucible classifient les comportements au niveau du noyau relatifs à la mémoire, aux processus et aux fichiers d'un outil d'extorsion, puis s'assurent qu'il correspond à l'une des capacités défensives connues. Occasionnellement, à l'image d'un vaccin, la formule peut être légèrement ajustée afin de produire une réponse plus précise.

Il est très rare que quelque chose de complètement nouveau apparaisse.

L'équipe de Cyber Crucible travaille de manière exhaustive pour découvrir de manière préventive des techniques nouvelles qui n'ont pas encore été observées au sein de notre clientèle, ni dans le renseignement sur les menaces.

L'effet ?

1. La défense contre les outils d'extorsion de Cyber Crucible est complète contre toutes les variantes connues de rançongiciels.

2. Les nouvelles variantes de rançongiciels sont bloquées avant même d'atteindre les premiers clients. Nous ne savons même pas comment nommer la plupart des logiciels contre lesquels nous

nous défendons pendant environ 120 jours, jusqu'à ce que les chercheurs « rattrapent leur retard ».

3. Les développeurs de rançongiciels et d'outils d'extorsion nous appellent parfois pour voir ce que nous préparons, afin de tenter de trouver un angle d'attaque. Malheureusement, la frustration causée par notre présence semble parfois stimuler leur évolution, ce qui rend d'autres outils encore moins efficaces.

4. Nous accueillons favorablement les tests de notre logiciel. Lorsque des testeurs d'intrusion, des analystes de logiciels malveillants ou des professionnels de l'émulation d'adversaires entament le processus commercial, cela nous enthousiasme !

Revision #1

Created 2026-07-24 07:02:56 UTC by Dennis Underwood

Updated 2026-07-24 07:02:56 UTC by Dennis Underwood